# Cyber security skills in the UK labour market 2021

## Technical report

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

Department for
Digital, Culture,
Media & Sport

Ipsos MORI

Ipsos

# Contents

# 1 Overview

The UK government Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos MORI and Perspective Economics to conduct research to improve their understanding of the current UK cyber security skills labour market. It builds on two comparable research studies which Ipsos MORI conducted for DCMS, published in 2020 (also in partnership with Perspective Economics)[1] and 2018.[2]

This report provides the technical details for all strands of the 2021 research, and copies of the main survey instruments (in the appendices) to help interpret the findings. DCMS has published a separate report of the main findings from the research.[3]

## 1.1 Full research objectives

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

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

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

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

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

## 1.2 Summary of methodology

The methodology consisted of four strands:

1. **Quantitative surveys –** Ipsos MORI conducted representative telephone surveys with 4 audiences: general businesses, public sector organisations, charities and cyber firms. These surveys gathered the main estimates on skills gaps and shortages reported in this study. Fieldwork was between 6 August and 30 October 2020.

2. **Qualitative interviews –** Ipsos MORI conducted a more focused strand of qualitative research, with 23 in-depth interviews split across large cyber firms, other medium and large businesses, and recruitment agents. The interviews explored the challenges these organisations faced in addressing skills gaps and shortages, and the approaches they were taking on recruitment, training and workplace diversity. Interviews took place across September and October 2020.

[1] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020.
[2] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.
[3] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021.

3. **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Burning Glass Technologies labour market database, showing the number, type and location of vacancies across the UK. This also covers remuneration, descriptions of job roles and the skills, qualifications and experience being sought by employers. This work primarily covered vacancies from September 2019 to the end of December 2020, supplementing the work done in the 2020 study (which covered vacancies from September 2016 to the end of August 2019).

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

## 1.3 Similarities and differences from the 2020 study

### Overall methodology changes and new audiences included in the research

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

- The 2018 and 2020 studies both included academic-led literature reviews to establish the existing evidence on cyber security skills gaps and shortages, and also to explore the approach that other countries outside the UK are taking to this issue (which is beyond the scope of the primary research). DCMS did not require a repeat literature review this year, as the evidence gathered in previous years was still considered relevant. However, to sense-check the findings from this study, the research team kept abreast of the major reports and statistics published in this area that covered the UK workforce, including:

  - Ongoing research on the cyber security recruitment pool, which Ipsos MORI is also carrying out for DCMS, to be published in 2021
  - DCMS's UK Cyber Security Sectoral Analysis 2021, which covers employment in the sector[4]
  - The Cybersecurity Workforce Study, which is an annual study by ISC2, a global membership organisation for cyber security professionals, with the latest version published in 2020[5]
  - The 2020 Cybersecurity Perception Study, also by ISC2[6]
  - The DCMS Sectors Economic Estimates, particularly those for earnings and employment, which are annually published Official Statistics, covering the UK digital sector[7]
  - The PwC Cyber Security Strategy 2021 report, which covered survey results with UK businesses and included a section on skills needs and hiring[8]

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

- The qualitative strand did not previously include recruitment agents – a new audience included for 2021. These interviews intended to explore the role of recruitment agents in the cyber security labour market in more depth. The same recruitment agent interviews also fed into the concurrent DCMS study on the cyber security recruitment pool, as the interview topics focused both on the

[4] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021.
[5] See https://www.isc2.org/Research/Workforce-Study. Before 2018, these were known as the Global Information Security Workforce Studies, or GISWS.
[6] See https://www.isc2.org/Research/Perception-Study#.
[7] See https://www.gov.uk/government/collections/dcms-sectors-economic-estimates.
[8] See https://www.pwc.co.uk/issues/cyber-security-services/insights/cyber-security-strategy-2021.html#explore.

demand side (in terms of employer demands and how employers work with agents) and the supply side (where agents found relevant job applicants and their own sense of the recruitment pool)

## Questionnaire changes

The quantitative survey questions are reviewed and partially revised each year to ensure we capture the metrics that are most useful for DCMS and its stakeholders. This year, we included questions on diversity in senior management roles, internships and staff turnover in the cyber sector. To make space for these questions, we removed questions from the previous surveys. The rationale for these removals is provided in Section 2.1.

The quantitative survey questions underwent cognitive testing in 2018. Although a small number of new questions have been added in later years, these have used tried-and-tested question wording wherever possible, so have not undergone cognitive testing. There has nonetheless been a live pilot of the quantitative survey each year, to pick up on any question comprehension problems (see Section 2.3).

## Sample sizes

The sample sizes achieved for each audience in the quantitative survey are slightly lower than 2020, except for charities. This year we interviewed:

- 965 businesses across other sectors (vs. 1,046 in 2020), of which 65 were large businesses (vs. 98 in 2020)
- 76 public sector organisations (vs. 106 in 2020)
- 220 charities (vs. 201 in 2020)
- 171 cyber firms (vs. 205 in 2020)

The survey fieldwork this year was heavily impacted by COVID-19 restrictions. Many organisations were less able or willing to take part in government surveys in general. Many were also no longer contactable by phone. In addition, among those that were contactable, it was not always feasible to reach the right senior individual responsible for cyber security in the organisation.

These small differences do not have a major impact on the overall reliability of the survey data. For example, the margins of error for the overall business samples are ±2-4 percentage points for both the 2021 and 2020 surveys.[9] The margin of error for large businesses has increased slightly (from ±6-11 percentage points in 2020 to ±8-13 percentage points in 2021). The sample sizes are still large enough to allow us to analyse the business results by size and sector.

COVID-19 and its impact on the survey are also likely to have affected the survey response rates, which we discuss in Section 2.4. However, we also do not expect this to have had any major detrimental impact on the reliability of the findings.

[9] The margins of error are confidence intervals at the 95% significance level, using the effective sample size. The effective sample size is a measure of the statistical reliability of samples that takes into account any sample manipulation such as weighting.

## 1.4 Differences from other recent studies looking at cyber security skills

### A note on the UK cyber security workforce size estimate from the 2020 Cybersecurity Workforce Study

ISC2 is a global membership organisation for cyber security professionals. It publishes an annual Cybersecurity Workforce Study, the most recent of which was published in November 2020.[10] This is a study of the global cyber security workforce and largely reports its findings at a global level.

The 2020 ISC2 report suggests there are c.366,000 individuals in the UK cyber security workforce, with a shortage of c.27,000. It is not possible for us to validate their estimate with our data, given the vast differences in methodologies between our two studies (outlined later in this section) and a lack of published technical information on the UK sample size and representativeness of the ISC2 data. The estimate is also likely to have a substantive margin of error around it.

DCMS's Cyber Sectoral Analysis 2021[11] estimates c.47,000 full-time employees working in cyber roles in the UK cyber sector, across the 1,481 cyber security companies that make up this sector. This excludes individuals working in cyber roles outside of these companies.

In our opinion, the ISC2 estimate is unrealistically high. It would mean that around 1 in 90 people in work in the UK are working in a cyber role. The DCMS Sectors Economic Estimates indicate that there were c.1.5 million jobs across all UK digital sectors in 2019.[12] If the ISC2 estimate was correct, this would mean that around 1 in 4 digital sector jobs are in cyber security.

### Broader comparability issues between this DCMS study and other studies on cyber security skills

The findings from the ISC2 2020 report touch on similar themes to our study (such as skills gaps, diversity in the cyber sector, qualifications and the impact of COVID-19) but they are not directly comparable. This is also the case for other well-known surveys that have been published since the previous DCMS cyber security skills study, including the PwC Cyber Security Strategy report.

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

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

- This research measures skills gaps – the number of organisations lacking specific cyber security skills – in a particular way. As we cannot objectively test whether organisations are capable of carrying out specific cyber security tasks involving specialist skills, we instead ask about their

[10] See https://www.isc2.org/Research/Workforce-Study.
[11] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021.
[12] See https://www.gov.uk/government/statistics/dcms-sectors-economic-estimates-2019-employment.

confidence at being able to carry out a range of these tasks (see Chapter 4 of the main report for full details). This continues the methodology from the 2 previous studies

## 1.5 Acknowledgements

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

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

We would also like to thank the Cyber Security Skills and Professionalisation Team at DCMS for their project management, support and guidance throughout the study.

# 2 Quantitative surveys

Ipsos MORI carried out all aspects of the quantitative surveys. This chapter provides technical details on the questionnaire development, sampling, piloting, main fieldwork and data processing.

## 2.1 Questionnaire development

Ipsos MORI developed the questionnaire and all the other survey instruments (such as the interviewer briefing notes, a reassurance email for respondents and a survey website page).

There were minimal changes in the questionnaire this year compared to the 2020 questionnaire. The changes reflected new or emerging themes that DCMS wished to gain further insight on, including new questions on:

- Diversity among senior staff in cyber roles in the cyber sector (Q20xa to Q20xe)
- The prevalence of internships or work placements in the cyber sector (Q47b)
- Staff turnover in the cyber sector, including the reasons for staff in cyber roles leaving their jobs (Q47x to Q47e)

Any new questions were typically added at the end of the relevant questionnaire section. The new section about staff turnover was added to the end of the existing questionnaire. This helped to avoid any order effects, which would limit the validity of trend data.

A number of the cyber firms interviewed for this study had also taken part in the earlier DCMS survey carried out in summer 2020, as part of the Cyber Sectoral Analysis 2021.[13] To avoid asking these firms to repeat the same information in this latest survey, the survey script included a question that collected permission for us to reuse the data from the earlier survey, thereby filtering this sample out of several firmographic questions (on the size of their total workforce and their cyber workforce specifically).

Appendix A includes a copy of the final questionnaire used in the main survey.

## 2.2 Sampling

The target population included:

- Private companies with more than one person on the payroll (i.e. excluding sole traders)
- Public sector organisations – mainly NHS organisations, academies and free schools (as other types of schools are run directly by local authorities) and local authorities (excluding parish councils)
- Registered charities
- Cyber sector businesses

We designed the survey to represent enterprises (i.e. the whole organisation) rather than establishments (i.e. local or regional offices or sites). This reflects that multi-site organisations will typically have connected cyber security infrastructure and will therefore deal with cyber security centrally.

[13] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021.

## Business and public sector sample frame (IDBR) and sample selection

The sample frame for businesses and public sector organisations was the government's Inter-Departmental Business Register (IDBR), which covers businesses in all sectors, including the public sector, across the UK at the enterprise level. This is the main sample frame for government surveys of businesses and for public sector organisations. Organisations in the agriculture, forestry and fishing sectors (SIC, 2007 category A) were excluded. DCMS judged cyber security to be a less relevant topic for these organisations, given their relative lack of e-commerce, and additional permission is needed to sample these organisations from the IDBR. This exclusion is consistent with the 2020 and 2018 studies.

In total, we selected 60,500 businesses and public sector organisations from the IDBR. This year we selected more leads than in 2020 (when it was 48,702) and 2018 (37,871), anticipating that COVID-19 restrictions would make fieldwork more challenging and require more sample to reach targets.

We selected leads based on disproportionate targets by sector and by size. The disproportionate stratification reflected the intention to carry out subgroup analysis by sector and size. This would not be possible with a proportionate stratification (which would effectively exclude any meaningful number of medium and large businesses from the selected sample, as well as resulting in too few interviews in certain sectors). The boosted groups included:

- Small (10 to 49 staff), medium (50 to 249 staff) and large size bands (250+ staff)
- Education businesses, finance or insurance businesses, manufacturing businesses, transport or storage businesses and public sector organisations (which DCMS highlighted as important sectors)
- Health, social care or social work businesses (which the 2018 literature review and subsequent research has suggested is a sector with a greater demand for cyber skills)
- Information or communication businesses (which are highly engaged with cyber security, according to findings from the separate DCMS Cyber Security Breaches Survey[14] series)

Table 2.1 breaks down the originally selected sample by size and sector. As the survey outcomes later in this chapter show, only 14,545 IDBR leads were included in the final survey, with the rest being unusable (i.e. with no telephone number) or being held in reserve.

**Table 2.1: Pre-cleaning selected IDBR sample by size and sector**

| SIC 2007 letter | Sector description | Micro or small (1–49 staff) | Medium (50–249 staff) | Large (250+ staff) | Total |
|---|---|---|---|---|---|
| B, C, D, E | Utilities or production (including manufacturing) | 1,667 | 159 | 284 | 2,110 |
| F | Construction | 5,737 | 70 | 48 | 5,855 |
| G | Retail or wholesale (including vehicle sales and repairs) | 2,606 | 191 | 251 | 3,048 |
| H | Transport or storage | 7,586 | 269 | 196 | 8,051 |
| I | Food or hospitality | 3,044 | 122 | 79 | 3,245 |
| J | Information or communications | 11,529 | 260 | 298 | 12,087 |
| K | Finance or insurance | 1,217 | 334 | 134 | 1,685 |
| L, N | Administration or real estate | 4,995 | 163 | 178 | 5,336 |
| M | Professional, scientific or technical | 6,836 | 137 | 157 | 7,130 |
| O | Other public sector | 101 | 148 | 314 | 563 |

[14] See https://www.gov.uk/government/collections/cyber-security-breaches-survey.

| SIC 2007 letter | Sector description | Micro or small (1–49 staff) | Medium (50–249 staff) | Large (250+ staff) | Total |
|---|---|---|---|---|---|
| P | Education (including academies) | 4,089 | 244 | 53 | 4,386 |
| Q | Health, social care or social work (including NHS) | 4,842 | 168 | 189 | 5,199 |
| R, S | Entertainment, service or membership organisations | 1,716 | 42 | 47 | 1,805 |
| | Total | 55,965 | 2,307 | 2,228 | 60,500 |

### Charity sample frames and sample selection

The target population of charities was all UK registered charities. The sample frames were the charity regulator databases in each UK country:

- The Charity Commission for England and Wales database: https://register-of-charities.charitycommission.gov.uk/register/full-register-download
- The Office of the Scottish Charity Regulator (OSCR) database: https://www.oscr.org.uk/about-charities/search-the-register/charity-register-download
- The Charity Commission for Northern Ireland database: https://www.charitycommissionni.org.uk/charity-search/

Again, this approach is consistent with the 2020 and 2018 study.

In England and Wales, and in Scotland, the respective charity regulator databases contain a comprehensive list of registered charities. The Charity Commission in Northern Ireland does not have a comprehensive list of established charities. It is in the process of registering charities and building one.

Therefore, while the Charity Commission in Northern Ireland database was the best sample frame for this survey, it cannot be considered as a truly random sample of Northern Ireland charities at present. This situation has, however, improved over time, as the database becomes more comprehensive.

This year, DCMS was granted full access to the non-public OSCR database, including telephone numbers, meaning we could sample from the full list of Scotland-based charities, rather than just those for which we were able to find telephone numbers.

The number of charity interviews was 220 (vs. 201 in 2020 and 470 in 2018). The sample was proportionately stratified by country and disproportionately stratified by income band. This stratification reflects the fact that the variance in survey responses tends to be higher among larger (high-income) charities, which increases the overall statistical reliability of the data.

As the entirety of the 3 charity regulator databases were used for sample selection, there was no restriction in the amount of charity sample that could be used, so no equivalent to Table 2.1 is shown for charities. In total, we sampled 1,417 charities to achieve 220 interviews.

### Cyber sector sample frame and sample selection

For cyber sector firms, we used the DCMS sector database that was created as part of the Cyber Sectoral Analysis 2021 (also carried out by Ipsos MORI and Perspective Economics). Perspective Economics built this sample frame, a list of 1,483 UK cyber sector firms, from the Orbis and Beauhurst databases. From this database, there were 965 records with telephone numbers.

All 965 leads were included in the survey. In other words, this survey was carried out using a census approach and achieved a simple random sample of 171 interviews.

### Sample telephone tracing and cleaning (required for IDBR sample)

Not all the original sample was usable. In total, 53,223 original business leads had either no telephone number or an invalid telephone number (i.e. the number was either in an incorrect format, too long, too short or a free phone number which would charge the respondent when called).

We carried out telephone matching through the DBS Data[15] (matching to both their business and, for micro businesses, residential number databases) to fill in the gaps where possible. This increases the amount of usable sample and helps to reduce the likelihood of non-response bias affecting the survey. There was already very high telephone coverage for charities from England and Wales (98% with telephone numbers), Northern Ireland (99% with telephone numbers) and Scotland (97% with telephone numbers). These provided more than enough usable sample and minimised the possibility of non-response bias. Therefore, no telephone matching was required for charities.

We also cleaned the selected sample to remove any duplicate telephone numbers, and parish councils. Identifying and removing parish councils was a two-step process. Firstly, we removed all micro organisations in SIC sector O from the usable sample, as these were overwhelmingly parish councils. Secondly, we carried out a search on the remaining SIC sector O organisations for the phrase “parish council”, “town council” or “community council” to highlight further leads for removal.

Following telephone matching and cleaning, the usable business sample amounted to 14,545 leads (i.e. 24% of the original sample frame). The composition of this sample is shown in Table 2.2.

[15] See https://dbsdata.co.uk/.

**Table 2.2: Post-cleaning available IDBR sample by size and sector**

| SIC 2007 letter | Sector description | Micro or small (1–49 staff) | Medium (50–249 staff) | Large (250+ staff) | Total |
|---|---|---|---|---|---|
| B, C, D, E | Utilities or production (including manufacturing) | 640 | 146 | 258 | 1,044 |
| F | Construction | 1,117 | 64 | 44 | 1,225 |
| G | Retail or wholesale (including vehicle sales and repairs) | 847 | 168 | 223 | 1,238 |
| H | Transport or storage | 962 | 253 | 172 | 1,387 |
| I | Food or hospitality | 655 | 105 | 68 | 828 |
| J | Information or communications | 1,377 | 207 | 244 | 1,828 |
| K | Finance or insurance | 728 | 292 | 113 | 1,133 |
| L, N | Administration or real estate | 848 | 140 | 157 | 1,145 |
| M | Professional, scientific or technical | 1,174 | 113 | 129 | 1,416 |
| O | Other public sector | 25 | 132 | 289 | 446 |
| P | Education (including academies) | 898 | 184 | 45 | 1,127 |
| Q | Health, social care or social work (including NHS) | 907 | 154 | 159 | 1,220 |
| R, S | Entertainment, service or membership organisations | 434 | 36 | 38 | 508 |
| | Total | 10,612 | 1,994 | 1,939 | 14,545 |

The usable leads for the survey were randomly allocated into separate batches for businesses and charities. Each batch included leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band, from previous Ipsos MORI surveys with these audiences, and from previous batches. In other words, we selected more sample in sectors and size bands where there was a higher target, or where response rates were expected to be relatively low.

We drew up and released subsequent batches of sample as and when the live sample was exhausted. All available leads were released in the main stage (see Tables 2.3, 2.4 and 2.5 for the total sample loaded).

The cyber sector sample did not require further telephone tracing or cleaning. This process had already been carried out in the previous survey conducted in summer 2020, as part of DCMS's Cyber Sectoral Analysis 2021.

## 2.3 Piloting

Much of the questionnaire remained unchanged nor involved rerouting existing questions again.

We conducted a live pilot for the surveys in the first 2 days of fieldwork (August 6 and August 7). This involved daily written feedback reports from all interviewers working on the project for those days, daily monitoring of raw survey data, interview lengths and sample outcomes, and an open-ended question at the end of the survey where respondents could give feedback.

We carried out 34 live pilot telephone interviews among the four audiences for the study (19 non-cyber sector businesses, 5 charities and 10 cyber sector businesses).

Following this year's live pilot, we only made minor changes to the questionnaire. This involved adding a new question (Q47x) for cyber sector businesses, to act as an initial filter question for the staff turnover section – this helped reduce the time taken in that section of the questionnaire. We also updated the reassurance email that can be sent to respondents within the survey script, to make it shorter and more user-friendly.

These 34 interviews were included in the final dataset, as the changes we made were not substantive enough to affect the comparability of findings before and after the pilot.

## 2.4 Fieldwork

All survey fieldwork (including the live pilot) was carried out from 6 August to 30 October 2020 using a Computer-Assisted Telephone Interviewing (CATI) script. This included a fieldwork extension of 3 weeks compared to the original timetable to counteract the impact that COVID-19 restrictions were having on participation. This is explained further in the response rate section (at the end of Section 2.4).

In total, we completed 1,432 telephone interviews, comprising:

- 965 businesses (excluding agriculture, forestry and fishing businesses and sole traders)
- 76 public sector organisations (excluding parish councils)
- 220 registered charities
- 171 cyber sector businesses

The average interview length was c.17 minutes for businesses, public sector organisations and charities and c.15 minutes for cyber firms. The average length for cyber firms was lowered by the fact that several had participated in the earlier cyber sectoral analysis survey (in summer 2020) so we did not need to collect their firmographic information again.

### Fieldwork preparation

Prior to fieldwork, the Ipsos MORI research team briefed the supervisory team for the telephone interviewers. The interviewers also received:

- Written briefing notes about all aspects of the survey
- A copy of the questionnaire and other survey instruments

### Screening of respondents

Interviewers used a screener section at the beginning of the questionnaire to identify the right individual to take part and ensure the business was eligible for the survey. At this point, the following organisations would have been removed as ineligible:

- Organisations with no computer, website or other online presence (interviewers were briefed to probe fully before coding this outcome, and it was used only in a handful of cases, for 1% of the released business sample and 4% of the released charity sample)
- Organisations that identified themselves as sole traders with no other employees on the payroll

As this was a survey of enterprises rather than establishments, interviewers also confirmed that they had called through to the UK head office or site of the organisation.

When an interviewer established that the organisation was eligible, and that this was the head office, we asked them to identify the senior member of staff who has the most knowledge or responsibility when it comes to cyber security. The briefing materials provided interviewers with a list of potential departments and job titles to ask for in non-micro businesses (e.g. IT Directors, Heads of Cyber Security and Chief Information Security Officers).

For UK businesses that were part of a multinational group, interviewers requested to speak to the relevant person in the UK who dealt with cyber security at the company level. In any instances where a multinational group had different registered companies in Great Britain and in Northern Ireland, both companies were considered eligible.

Franchisees with the same company name but different trading addresses were also all considered eligible as separate independent respondents.

### Random-probability approach and maximising participation

We adopted random-probability sampling and interviewing to minimise selection bias. The overall aim with this approach is to have a known outcome for every piece of sample released. For this survey, we used an approach comparable to other robust business surveys and to the 2020 and 2018 studies:

- We called each piece of sample either a minimum of 7 times, or until we achieved an interview, received a refusal, or received enough information to make a judgment on the eligibility of that contact. Typically, we called leads 10 or more times (e.g. when respondents had requested to be called back at an early stage in fieldwork but had subsequently not been reached)

- Each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. We also offered evening and weekend interviews on request to respondents

Several steps were taken to maximise participation in the survey and reduce non-response bias, beyond the general management and scheduling of the fieldwork and interviewing team to produce the best results. Interviewers could send a reassurance email to prospective participants to confirm the legitimacy of the study and provide more information. We also had a study website and GOV.UK page to reassure respondents that this was a bona fide government survey. We also offered respondents a copy of the previous year’s report and a government cyber security help card, sent immediately at the end of the interview if they took part. The help card included up-to-date government guidance (from the National Cyber Security Centre) for organisations on cyber security in general and specifically for the COVID-19 pandemic (both reproduced in Appendix B) to encourage participation.

### Additional steps taken in light of COVID-19 restrictions

In anticipation of the impact of COVID-19 on participation in the survey, we also took a number of extra steps this year to improve the sample coverage and the response rate, including:

- Manual sample improvement, focused on the large business and cyber sector samples, where members of the research team looked up relevant employee names and job titles, email addresses and alternative phone numbers on Google, LinkedIn and company websites
- Additional matching for medium, large and cyber sector businesses to existing board-level contacts and email addresses on the DBS Data
- Hosting a freephone telephone number and project-specific email inbox that allowed respondents to reply and set up their own appointments, or take part in the survey there and then

With the collected email addresses, the research team sent out a mass mailing to encourage respondents to reply and set up an appointment, or to correct the contact information we had in the sample for their organisation. In total, we sent 86 emails to large businesses and 87 to cyber firms.

## Fieldwork monitoring

Ipsos MORI is a member of the interviewer Quality Control Scheme recognised by the Market Research Society. In accordance with this scheme, the field supervisor on this project listened in on at least 10 per cent of the interviews and checked the data entry on screen for these interviews. The Ipsos MORI core research team also listened in during the early interviews and gave further feedback to the telephone interviewers on how to best introduce the survey.

## Fieldwork outcomes and response rate

The Ipsos MORI research team monitored fieldwork outcomes and response rates throughout fieldwork and gave interviewers regular guidance on how to avoid common reasons for refusal. Table 2.3 shows the final outcomes and the adjusted response rate calculation for business and public sector (the IDBR sample). Tables 2.4 and 2.5 shows the equivalent for charities and cyber firms.

Compared to 2020 and 2018, the unadjusted response rate is lower for the IDBR sample (9% this year, vs. 11% in 2020 and 14% in 2018) and for charities (15% this year, vs. 36% in 2020 and 30% in 2018). Compared to 2020, the unadjusted response rate for the cyber sample is also lower (18% vs. 22%).

The lower response rates are likely to be due to a combination of unique circumstances brought about by the COVID-19 restrictions, as well as the ongoing challenge of declining response rates in survey fieldwork in general. This survey's fieldwork took place just before and during the second wave of COVID-19 infections in the UK and while various COVID-19 restrictions affecting the business population were in place. These restrictions and the overall environment under which fieldwork took place meant:

- It was harder to reach organisations via landline numbers as many switchboards were no longer running or had a skeleton service
- When we did get through, it was harder to reach the right individual within the organisation, who may have been working remotely rather than in an office, or may have been placed on furlough (which was the case with 3% of businesses and 3% of charities)
- Where we did reach the right person, these individuals were often busier than before and less willing to take part in surveys in general

More generally, there has been an increasing awareness of cyber security, potentially making businesses more reticent to take part in surveys on this topic.

**Table 2.3: Fieldwork outcomes and response rate calculations for businesses and public organisations (IDBR sample)**

| Outcome | Total |
|---:|---|
| Total sample released | 11,642 |
| Completed interviews | 1,041 |
| Incomplete interviews | 54 |
| Ineligible leads – established during screener[16] | 170 |
| Ineligible leads – established pre-screener | 155 |
| Refusals | 1,710 |

[16] Ineligible leads were those found to be sole traders, public sector organisations or the small number of organisations that self-identified as having no computer, website or online interaction. Those falling in the latter self-identified category were probed by interviewers to check this was really the case.

| Outcome | Total |
|---:|---|
| Unusable leads with working numbers[17] | 1,221 |
| Unusable numbers[18] | 1,239 |
| Working numbers with unknown eligibility[19] | 6,052 |
| Expected eligibility of screened respondents[20] | 87% |
| Expected eligibility of working numbers[21] | 59% |
| Unadjusted response rate | 9% |
| Adjusted response rate | 17% |

### Table 2.4: Fieldwork outcomes and response rate calculations for charities

| Outcome | Total |
|---:|---|
| Total sample released | 1,417 |
| Completed interviews | 220 |
| Incomplete interviews | 10 |
| Ineligible leads – established during screener | 8 |
| Ineligible leads – established pre-screener | 55 |
| Refusals | 137 |
| Unusable leads with working numbers | 202 |
| Unusable numbers | 101 |
| Working numbers with unknown eligibility | 684 |
| Expected eligibility of screened respondents | 97% |
| Expected eligibility of working numbers | 79% |
| Unadjusted response rate | 15% |
| Adjusted response rate | 29% |

### Table 2.5: Fieldwork outcomes and response rate calculations for cyber firms

| Outcome | Total |
|---:|---|
| Total sample released | 965 |
| Completed interviews | 171 |
| Incomplete interviews | 2 |
| Ineligible leads – established during screener | 0 |
| Ineligible leads – established pre-screener | 1 |
| Refusals | 152 |

[17] This includes sample where there was communication difficulty making it impossible to carry out the survey (either a bad line, or language difficulty), as well as numbers called 10 or more times over fieldwork without ever being picked up.

[18] This is sample where the number was in a valid format, so was loaded into the main survey sample batches, but which turned out to be wrong numbers, fax numbers, household numbers or disconnected.

[19] This includes sample that had a working telephone number but where the respondent was unreachable or unavailable for an interview during the fieldwork period, so eligibility could not be assessed.

[20] Expected eligibility of screened respondents has been calculated as: (completed interviews + incomplete interviews) / (completed interviews + incomplete interviews + leads established as ineligible during screener). This is the proportion of refusals expected to have been eligible for the survey.

[21] Expected eligibility of working numbers has been calculated as: (completed interviews + incomplete interviews + expected eligible refusals) / inactive leads with working numbers).

| Outcome | Total |
|---:|---|
| Unusable leads with working numbers | 129 |
| Unusable numbers | 31 |
| Working numbers with unknown eligibility | 479 |
| Expected eligibility of screened respondents | 100% |
| Expected eligibility of working numbers | 83% |
| Unadjusted response rate | 18% |
| Adjusted response rate | 26% |

### Expected negligible impact of lower response rates

It is important to remember that response rates are not a direct measure of non-response bias in a survey, but only a measure of the potential for non-response bias to exist. Previous research into response rates, mainly with consumer surveys, has indicated that they are often poorly correlated with non-response bias.[22]

The idea of non-response bias entering the survey assumes that the organisations declining to take part are substantially different in terms of their cyber skills needs to the ones we did interview. If we believe, reasonably, that the response rates this year were mainly lower due to COVID-19 and associated restrictions, then we must consider whether the businesses most negatively impacted by COVID-19 are likely to have different cyber skills needs and challenges – we have no strong reasons to believe this.

## 2.5 Data processing and weighting

### Identifying the type and characteristics of sampled organisations using sample information versus questionnaire information

The IDBR contains businesses that might also be registered charities. Moreover, the public sector organisations within the IDBR sample are split across several sectors (most commonly SIC 2007 sectors P, Q and O[23]), so cannot be fully identified at the sampling stage. We allowed all IDBR-sampled organisations to self-identify as either a private sector organisation, public sector organisation or charity in the interview. We then took this as their designated status in the final data.

For size (or income band for charities), we primarily used information collected in the questionnaire, and where this was missing, we used the information in the sample frames to fill in the missing responses.

### Coding

The verbatim responses to unprompted questions could be coded as “other” by interviewers when they did not appear to fit into the predefined code frame. Ipsos MORI’s coding team coded these “other” responses manually, and where possible, assigned them to codes in the existing code frame. It was also possible for new codes to be added where enough respondents – 10 per cent or more – had given a similar answer outside of the existing code frame. The accuracy of the coding was verified by the Ipsos MORI research team, who checked and approved each new code proposed.

[22] See, for example, Groves and Peytcheva (2008) “The Impact of Nonresponse Rates on Nonresponse Bias: A Meta-Analysis”, Public Opinion Quarterly (available at: https://academic.oup.com/poq/article-abstract/72/2/167/1920564) and Sturgis, Williams, Brunton-Smith and Moore (2016) “Fieldwork Effort, Response Rate, and the Distribution of Survey Outcomes: A Multilevel Meta-analysis”, Public Opinion Quarterly (available at: https://academic.oup.com/poq/issue/81/2).
[23] The definitions for these SIC letters is in Table 4.1.

We did not undertake SIC coding. Instead, we used the SIC 2007 codes that were already in the IDBR sample to assign businesses to a sector for weighting and analysis purposes. This is the same approach as in both 2020 and 2018 survey and has been tested and validated in previous surveys, such as DCMS's Cyber Security Breaches Survey series.[24] The sector groupings used in the main report match those shown in Tables 2.1 and 2.2.

## Weighting

For the IDBR and charity samples, we applied RIM weighting (Random Iterative Method weighting) to account where possible for non-response bias, and to account for the disproportionate sampling by size, sector and income band. The intention was to make the final reported data representative of the actual UK business, public sector and charity populations. This matched the weighting approaches from the 2018 and 2020 studies.

RIM weighting is a standard weighting approach undertaken in business surveys of this nature. In cases where the weighting variables are strongly correlated with each other, it is potentially less effective than other methods, such as cell weighting. However, this is not the case for this survey as organisation size and sector are not correlated.

We used 4 separate weighting schemes:

1. For businesses, there were non-interlocking weights by size and sector, based on the population profile in the 2020 Department for Business, Energy and Industrial Strategy (BEIS) business population estimates (the latest ones published at the time of data processing).[25] Non-interlocking weighting means that we did not weight by size *within* each sector, but weighted the whole sample separately by size and then by sector. Interlocking weighting (i.e. weighting by size band within each sector) was also possible but would have potentially resulted in very large weights. This would have reduced the statistical power of the survey results without making any considerable difference to the weighted percentage scores for each question, so was not applied.

   We did not weight by region, but it should be noted that the final weighted data is closely aligned with the regional profile of the population.

2. For charities, we used non-interlocking weights by income band and country. We took the profile in the charity regulator databases (including the leads that could not be used in the survey) as the definitive population profile.

3. For public sector organisations, we also weighted based on the public sector profile in the 2020 BEIS business population estimates.

4. One complexity in the weighting of private and public sector organisations is that certain sectors of the economy contain a mix of the private and public sector – especially education (SIC sector P) and health (SIC sector Q). For analysing these 2 sector subgroups, we created a fourth weighting scheme that merged the private and public sector population profiles from the 2020 BEIS estimates.

We have not weighted the cyber sector sample. This is because:

[24] See https://www.gov.uk/government/collections/cyber-security-breaches-survey.

[25] See https://www.gov.uk/government/collections/business-population-estimates.

- There was no disproportionate sampling for this survey sample, so corrective weights were not needed
- We compared the profile by size band achieved in this survey to the profile from the earlier Cyber Sectoral Analysis 2021 survey,[26] which was also not weighted. This is the best comparison to indicate whether the sample is skewed in any way. Both surveys broadly achieved the same profile
- There is no other reliable profile data on the sector

Tables 2.6 to 2.8 show the unweighted and weighted profiles of the data.

### Table 2.6: Unweighted and weighted sample profiles for businesses (excluding industry sectors that contain both private and public sector organisations)

| | Unweighted % | Weighted % |
|---|---|---|
| Size | | |
| Micro or small (1–49 staff) | 81% | 97% |
| Medium (49–249 staff) | 13% | 3% |
| Large (250+ staff) | 9% | 1% |
| Sector | | |
| Administration or real estate | 8% | 13% |
| Construction | 7% | 13% |
| Entertainment, service or membership organisations | 2% | 7% |
| Finance or insurance | 8% | 2% |
| Food or hospitality | 5% | 10% |
| Information or communications | 11% | 6% |
| Professional, scientific or technical | 10% | 14% |
| Retail or wholesale | 12% | 18% |
| Transport or storage | 9% | 4% |
| Utilities or production (including manufacturing) | 11% | 7% |
| Region | | |
| East Midlands | 7% | 7% |
| Eastern | 10% | 10% |
| London | 15% | 12% |
| North East | 2% | 2% |
| North West | 10% | 9% |
| Northern Ireland | 4% | 5% |
| Scotland | 8% | 10% |
| South East | 16% | 16% |
| South West | 9% | 10% |
| Wales | 4% | 4% |
| West Midlands | 8% | 9% |
| Yorkshire and Humberside | 7% | 8% |

[26] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021.

**Table 2.7: Unweighted and weighted sample profiles for charities**

| | Unweighted % | Weighted % |
|---|---|---|
| Income band[27] | | |
| £0 to under £100,000 | 46% | 76% |
| £100,000 to under £500,000 | 15% | 15% |
| £500,000 or more | 37% | 8% |

**Table 2.8: Unweighted and weighted sample profiles for public sector organisations (using independent weighting scheme) and industry sectors that contain both private and public sector organisations (using merged weighting scheme)**

| | Unweighted % | Weighted % |
|---|---|---|
| Size | | |
| Micro or small (1–49 staff) | 39% | 26% |
| Medium (49–249 staff) | 32% | 47% |
| Large (250+ staff) | 29% | 25% |
| Sector | | |
| Education (including academies) | 10% | 2% |
| Health, social care or social work (including NHS) | 9% | 4% |

## 2.6 Workforce-level estimates

The following figures in the report are workforce-level estimates rather than employer-level estimates. That is, they show findings as a proportion of the cyber workforce, rather than as a proportion of employers:

- Career pathways into cyber roles outside the cyber sector (Figure 2.3 in the findings report)
- Career pathways into cyber roles in the cyber sector (Figure 2.4)
- Diversity estimates in the cyber sector (Figure 3.1)
- Staff turnover estimates in the cyber sector (Section 8.1)

A further figure in the report is calculated as a proportion of all vacancies, rather than as a proportion of all employers with vacancies:

- The proportion of all cyber sector vacancies that are hard-to-fill (Section 6.3)

In all cases, these are weighted estimates, which account for the different number of people working in cyber roles in each organisation sampled in the survey.

Individual outliers in the data can heavily affect these estimates. Therefore, there were two stages of checking for outliers. Firstly, the survey script included soft checks that forced interviewers to revalidate unusually high numeric answers from the respondent (e.g. an unusually high number of employees with neurodiverse conditions or learning disorders) before moving on to the next question. Secondly, the research team manually checked the final data for outliers and recalculated the estimates without these outliers, in order to check the impact they were having on answers. This led to us removing two outliers:

[27] For just under 2 per cent of the charities interviewed, income status was unknown, and these were not weighted by income.

- For calculating the proportion of all staff in cyber roles that have neurodiverse conditions or learning disorders (Figure 3.1), we removed a single outlier where a cyber sector business with 5-500+ employees said that more than a quarter of them were neurodivergent
- For calculating the proportion of all cyber sector vacancies that are hard-to-fill, we removed a single outlier where a cyber sector business with 40+ vacancies said they were all hard-to-fill

## 2.7 Rounding of percentages from the survey estimates

In the findings report, the survey data are rounded up to whole percentages. Therefore, in some cases, charts will appear to add to slightly more than 100%. For example, if the calculated estimates for a question are 20.6%, 40.7% and 38.7%, they will show as 21%, 41% and 39%.

# 3 Qualitative interviews

As well as the survey, Ipsos MORI conducted 23 qualitative in-depth interviews in September and October 2020. This included:

- 9 cyber sector businesses
- 8 medium and large organisations from other sectors (1 with 50+ staff 7 with 250+ staff)
- 6 recruitment agents (5 were specialist cyber recruitment agents and 1 was a generalist recruitment agent that recruited for these and other roles)

The data collected in the recruitment agent interviews also informed another DCMS study that Ipsos MORI is carrying out on the UK cyber security recruitment pool.

The focus on larger organisations reflects the fact that:

- Larger organisations tend to have more sophisticated cyber security needs and are therefore likely to have more acute cyber security skills challenges
- The sample of large organisations achieved in the quantitative survey is relatively small, so it became more important to explore this audience in the remaining research strands

## 3.1 Sampling and recruitment

### Cyber sector businesses and large organisations

The cyber firms and other medium and large organisations were recruited from the survey. The sampling was purposive – Ipsos MORI identified the best organisations to recruit based on their survey responses, with quotas applied to recruit those that had advanced skills needs, hard-to-fill job vacancies, carried out relevant training for those in cyber roles or wider staff, taken action to improve their workforce diversity and had staff recently leaving the organisation.

Survey respondents gave permission to be recontacted in the survey. Our specialist recruitment team then emailed and telephoned these respondents inviting them to take up in this follow-up strand. We offered a £50 thank you payment or charity donation to each participant to encourage participation.

### Recruitment agents

We sampled recruitment agents in two ways:

- The Ipsos MORI team carried out desk research to find people recruiting for cyber roles online that might be suited to the research. In total, 4 of the 6 interviews were achieved from this approach
- We also carried out snowball recruitment, which involved asking those that had already participated for any other contacts they might have who could also take part

In both cases, we approached these potential participants via email and, upon them agreeing to take part, administered a screener by telephone to ensure they were eligible. The screener asked about the length of time they had been recruiting for these roles and how often they recruited them. We offered a £100 thank you payment or charity donation to each participant to encourage participation, with the higher incentive in this case (relative to those recruited from the survey) reflecting that we were cold contacting these participants.

## 3.2 Fieldwork

The Ipsos MORI research team carried out each interview either over the telephone or virtually via Microsoft Teams. Each interview with cyber firms and other medium and large organisations lasted c.60 minutes. The interviews with recruitment agents were longer, at c.90 minutes – this reflected the fact that we were exploring both the demand side (in terms of employer relationships, needs and demands) and the supply side (in terms of the recruitment pool, for the sister DCMS project on this topic).

The topics for discussion were agreed collaboratively between Ipsos MORI and DCMS. Ipsos MORI wrote these up in a topic guide that DCMS approved for use. As a summary, the topics covered in the large organisation and cyber firm interviews included:

- The nature of cyber security skills gaps and the challenges of addressing these
- Training approaches and challenges (both for those in cyber roles and wider staff)
- Recruitment approaches and challenges, including working with recruitment agents and HR colleagues
- Perceptions of workforce diversity and actions taken in this area
- The impact of COVID-19 across all these topics

The topics covered in the recruitment agent interviews were:

- Their applicant pool, and where and how they source applicants
- The diversity of the applicant pool
- Employers' recruitment criteria
- Approaches to recruitment and keeping up to date with industry needs
- The impact of COVID-19 across all these topics

The full topic guides for each audience are included in Appendices C and D.

## 3.3 Analysis

Interviews were summarised in an Excel notes template and also recorded for analysis purposes. Throughout fieldwork, the core research team verbally discussed interim findings and outlined areas to focus on in subsequent interviews. DCMS also attended one of these discussions. At the end of fieldwork, we drew out key themes, examples and anonymised quotes to include in the final findings.

# 4 Job vacancies analysis

Perspective Economics led this strand of the research. While it was carried out concurrently with the quantitative survey, the job data included in the analysis follows on from last year's research. The new data for this year focuses on the 2020 calendar year (1 January to 31 December). The data in the previous study covered the period from 2016 to 2019, i.e. 3 years of data. Therefore, across both years of the study that have adopted this methodology, we have over 4 years of trend data to examine.

The analysis approach is consistent with last year's research, which enables us to look at trends over time in the demand for cyber professionals in the UK labour market.

## 4.1 Methodology

### The Burning Glass Technologies definition of cyber job roles

Burning Glass Technologies[28] has been tracking the cyber security job market since 2013. Its database has a basic filter for cyber security job postings based on job titles, required skillsets and certifications. This filter broadly covers, but does not distinguish between, roles that Burning Glass Technologies defines as "core" and "cyber-enabled". The difference between the two, adapted from the Burning Glass Technologies definition[29], is as follows:

- 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 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, other than those already mentioned, include Computer Support, IT Support Analyst and Applications Analyst

It is important to note that both sets of job roles typically require a mix of technical and non-technical cyber security skills, so these cannot simply be differentiated as technical vs. non-technical jobs in cyber security.

[28] This work was carried out using the Burning Glass Technologies Labour Insight tool: https://www.burning-glass.com/products/labor-insight/.

[29] See https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf.

## Improving on the Burning Glass Technologies standard cyber security filter

Using the Burning Glass Technologies cyber security filter suggests that there were 69,676 cyber security job postings in the UK between in 2020. However, we know that this filter is incomplete for the purposes of our analysis:

- It is important to have a more granular split between core and cyber-enabled roles. While the Burning Glass Technologies filter aims to cover both, it does not distinguish between the two

- Furthermore, it is common for cyber security job titles to have multiple or inconsistent meanings within the cyber sector and across sectors. For example, a “Security Lead” could refer to cyber security or to physical security. A “Risk Analyst” could refer to someone in cyber security or in the finance sector. This means that the Burning Glass Technologies filter could both exclude jobs that are cyber security jobs (false negatives) and include jobs that do not, in fact, include any cyber functions (false positives)

Both for this year’s study and the previous 2020 study, Perspective Economics has sought to identify cyber security job postings in the UK using a more tailored and systematic approach than is applied by Burning Glass Technologies’ standard filter. Our approach has clear inclusion and exclusion criteria and can be replicated. We sought to exclude common words and roles that might generate misleading findings, e.g. removing words such as “financial”, “fire” or “CCTV” (indicating a different type of analyst or security role). We also excluded roles that mentioned “cyber security” but would be unlikely to employ core or cyber-enabled skillsets, such as sales, recruitment or human resources roles.

In order to develop this approach, we undertook the following iterative steps:

1. Initial identification of more granular search terms to use on the Burning Glass Technologies platform (which we aligned to the Cyber Security Body of Knowledge, or CyBOK[30]).
2. Extracting an initial dataset from Burning Glass Technologies with granular level job postings, using the identified inclusion/exclusion terms from step 1.
3. Reviewing the initial output and refining the inclusion/exclusion terms before extracting a second dataset from Burning Glass Technologies using the refined terms.
4. Supplementing the second dataset with Burning Glass Technologies’ own cyber security filter, which we used to distinguish between core cyber roles and cyber-enabled roles.
5. Confirming the final number of job postings within scope for this analysis (using the final, refined search strategy) with DCMS.

Whilst these steps have remained consistent across both the 2020 and 2021 studies, we have reviewed the job titles within 2020 job postings, and removed any notable anomalies. For example, this year, we remove trainee positions whereby there is no clear known employer, e.g. an advertisement for a cyber security training programme with no known job outcome.

In 2020, our revised search criteria yielded 33,528 core cyber security roles, and a further 59,912 cyber-enabled roles. In total this comes to 93,450 job postings in scope for this strand (compared to Burning Glass Technologies’ own 69,676 job postings yielded from the cyber security filter).

We have included the final inclusion/exclusion criteria in Appendix E.

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

## 4.2 Metrics analysed

The analysis took advantage of the following data outputs from the Burning Glass Technologies database:

- The number of cyber security job postings in the UK, including a time-series analysis of the number of job postings posted each month over the last year
- The industry sectors of the employers seeking people in cyber roles
- The geographic locations across the UK for these job postings
- Advertised job titles (to analyse the job roles most in demand)
- Job descriptions (to analyse the skills, experience, education, and qualifications being requested)
- The salaries or salary ranges being offered in these job postings

The analysis of the overall number of job postings also considers the changes in the market over the course of the COVID-19 pandemic. The separately published findings report includes a comparison between cyber security roles, digital roles, and the broader UK labour market (in terms of the decline and recovery in job postings).[31]

## 4.3 Strengths and limitations of the methodology

This methodology adds a great deal of insight to the quantitative survey data, particularly around the geographical clustering of job postings. It also reinforces the survey findings in many areas, adding another layer of credibility to this data.

A summary of the advantages of this approach is as follows:

- **Volume and granularity** – we are able to analyse over c. 620,000 job postings from the last five years, exploring the specific jobs, skills, and qualifications in demand. It can also drill down into areas such as the specific coding languages being sought. This method can uncover geographic clustering (down to specific towns and cities) of high demand and skills shortages for cyber professionals

- **Real-time analysis** – the highly up-to-date data on Burning Glass Technologies can provide insight into the labour market at that given moment in time. By contrast, survey statistics and other secondary data are typically several months or years old, and they are not regularly updated. This is especially important given the fast-moving nature of cyber security and the evolving demand for skills

- **Strong coverage** – the Burning Glass Technologies platform scrapes more than 40,000 online data sources[32]. Online postings reflect an estimated 85 per cent of jobs posted in the labour market (versus, e.g. print media)

However, the findings are based solely on job postings recorded on the Burning Glass Technologies platform. This means that the data comes with the following limitations:

- **Selection bias** – Burning Glass Technologies only scrapes free-to-use jobsites, which potentially leaves an (unknown) risk of bias if major employers are using closed platforms to post jobs, or other ways of recruiting such as networking and word-of-mouth. However, we believe this is offset

[31] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021.
[32] See https://www.burning-glass.com/about/faq/.

by both the high volume and high coverage of the data that is available. This data still gives a strong insight into the trends and patterns in the labour market

- **Interpretation of job roles –** the Burning Glass Technologies interpretation of cyber security jobs is reliant upon their definition, based on the skills, job titles and qualifications expected for cyber roles. There is a risk that some roles within their interpretation may not truly be considered a cyber role (e.g. administrative staff working in the NHS responsible for document shredding, flagged as “Information Security”). This is the most substantial risk associated with this methodology and is why we have opted not to use the Burning Glass Technologies filter for our analysis, but instead to adopt a more bespoke search strategy, with the tailored inclusion/exclusion terms. These search terms reduce the risk of including non-cyber roles (false positives) within the analysis

## 4.4 Presentation of percentages

In the findings report, we typically show the percentages from the job vacancies analysis to 1 decimal place. This is because, unlike the survey estimates, they are based on the entirety of the secondary dataset, rather than a survey sample – they are, therefore, not estimates with margins of error.

Some of the metrics covered by the Burning Glass dataset will have varying sample sizes. For example, whilst all roles will have a job title, there are other measures that can be less complete such as salary brackets or employer (where the advertisement is through a recruiter). Where the sample size is lower than the number of job postings, we set out the size of the underlying sample for each measure accordingly (i.e. in any charts).

# 5 Recommendations workshop

Ipsos MORI hosted a virtual workshop on Adobe Connect in November 2020. The organisations represented at the workshop were DCMS, the Cabinet Office, the National Cyber Security Centre (NCSC) and some of the organisations that are part of the Cyber Security Alliance, working on the UK Cyber Security Council Formation Project.[33] Ipsos MORI's study partners also attended, namely Sam Donaldson from Perspective Economics, David Crozier from the Centre for Secure Information Technologies and Professor Steven Furnell from University of Nottingham.

The purpose of the workshop was to help cocreate a set of recommendations from this year's study.

Workshop participants first received a presentation of the key findings from the primary and secondary research. Ipsos MORI then facilitated a series of breakout discussion groups on the main research topics: skills gaps, training and qualifications, recruitment and retention, and workforce diversity. For context, all participants received a copy of the 15 recommendations from last year's study.

Ipsos MORI used the notes from these breakout discussions to inform this year's draft recommendations, which were all based on evidence generated from the primary and secondary research strands. The DCMS project team approved the final set of recommendations.

[33] See https://www.theiet.org/impact-society/uk-cyber-security-council-formation-project/.

# Appendix A: 2021 questionnaire

INTERVIEWER INSTRUCTIONS IN CAPS
ROUTING/SCRIPTING/TEXT SUBSTITUTION INSTRUCTIONS (I.E. EVERYTHING THAT WILL NOT APPEAR ON THE INTERVIEWER SCREEN) IN RED CAPS

GENERAL BUSINESSES OR PUBLIC SECTOR (SAMPLE S_TYPE=1)
CHARITIES (SAMPLE S_TYPE=2)
CYBER SECTOR BUSINESSES (SAMPLE S_TYPE=3)

## Introduction

Is this the head office for [SAMPLE S_CONAME]?

IF NOT THE HEAD OFFICE, ASK TO BE TRANSFERRED AND RESTART

Hello, my name is … from Ipsos MORI, the independent research organisation. We are conducting a survey on behalf of the UK Government Department for Digital, Culture, Media and Sport about cyber skills. This is an annual survey used to collect government statistics. It is relevant for all types of organisations.

SAMPLE S_FREENUMTEXT

SAMPLE S_RESPTEXTSUB

Would you be happy to take part in an interview? This should take around 15 minutes for the average organisation, and will be shorter for smaller organisations.

ADD IF NECESSARY:

- The survey will help inform government policy on how it can best help organisations like yours to address their skills and recruitment needs.
- As a thank you, we can send you an infographic summary of last year's findings, and a government help card with the latest official cyber security guidance for organisations, including guidance on staying secure under COVID-19. These would get emailed to you as soon as you complete the survey.

ADD DEFINITION OF CYBER SECURITY IF NECESSARY:

- By cyber security, I mean any strategy, processes, practices or technologies that organisations have in place to protect their networks, computers, programs, the data they hold, or the services they provide, from unauthorised access, harm or misuse.

REASSURANCES IF NECESSARY:

- Details of the survey are on the GOV.UK website at https://www.gov.uk/government/publications/cyber-security-labour-market-research
- You can also Google the term "Understanding the UK cyber security labour market" to find the same link yourself.
- SAMPLE S_INTROTX

## Reassurance email

Wants more information by email SEND REASSURANCE EMAIL
SHOW ALL OTHER STANDARD OUTCOME CODES PLUS THE FOLLOWING BESPOKE OUTCOME CODES:

- 170 refused – outsources cyber security
- 171 soft refusal
- 172 refused – no cyber security issues/problems
- 173 refused – think survey is not genuine
- 174 refused – company no-name policy
- 175 refused – cyber security is commercially confidential
- 176 – right respondent unavailable due to COVID-19
- 180 – wrong direct line
- 181 – duplicate business
- 201 ineligible – sole trader at SIZEA
- 247 ineligible – no computer, website or online use
- 249 ineligible – sole trader at intro

## Consent

ASK ALL
**Q1w.CONSENTA**
Before we start, I just want to clarify that participation in the survey is confidential and voluntary. Results of the survey will be anonymised and not attributable to you. You can change your mind at any time. Are you happy to proceed with the interview?

If you would like to read the privacy policy before we continue, I can give you the link. If you're happy to proceed we'll continue.
ADD IF NECESSARY: You can access the privacy policy on our website at: https://ipsos.uk/12025p

SINGLE CODE
Yes
No
CODE 2 CLOSES SURVEY

ASK IF CYBER SECTOR BUSINESS (SAMPLE S_TYPE=3)
**Q1y.CONSENTC**
Your business may have taken part in an Ipsos MORI survey for DCMS in May, June or July 2020, which was about understanding the UK cyber sector. We can reuse your answers from that survey in this one to make it much shorter. To do this, we would have to match your business details across both surveys. Are you happy for us to do this?
INTERVIEWER NOTE: IF THEY SAY NO, REITERATE THAT THIS IS SO WE CAN AVOID ASKING THEM TO REPEAT THEIR ANSWERS IN THE PREVIOUS SURVEY.

SINGLE CODE
Yes – reuse
No – don't reuse
Didn't take part in previous survey

DUMMY VARIABLE NOT ASKED
**Q1z.CONSENTCDUM**

SINGLE CODE
IF TOOK PART IN SECTORAL ANALYSIS AND GIVE CONSENT FOR DATA LINKING (SAMPLE S_SECTORAL=1 AND CONSENTC CODE 1): Skip questions
OTHERWISE (SAMPLE S_SECTORAL=2 OR CONSENTC CODES 2 OR 3): Do not skip questions

## Organisational profile

READ OUT IF NOT SKIPPING QUESTIONS (CONSENTCDUM NOT CODE 1)
First, some questions about your organisation as a whole.

ASK IF BUSINESS OR PUBLIC SECTOR (SAMPLE S_TYPE=1)
**Q1.TYPEX**
Is your organisation … ?
READ OUT
INTERVIEWER NOTE: IF THEY HAVE A SOCIAL PURPOSE BUT STILL MAKE A PROFIT (E.G. PRIVATE PROVIDER OF HEALTH OR SOCIAL CARE) CODE AS CODE 1

SINGLE CODE
Mainly seeking to make a profit
A social enterprise
A charity or voluntary sector organisation
A government-financed body or public sector organisation
DO NOT READ OUT: Don't know

DUMMY VARIABLE NOT ASKED
**Q1a.TYPEXDUM**
Is your organisation … ?

SINGLE CODE

IF SAMPLE S_TYPE=1 AND TYPEX CODES 1, 2 OR DK: Private sector
IF SAMPLE S_TYPE=2 OR TYPEX CODE 3: Charity
IF SAMPLE S_TYPE=1 AND TYPEX CODE 4: Public sector
IF SAMPLE S_TYPE=3: Cyber sector

SCRIPT TO BASE BUSINESS/CHARITY [director/trustee] AND [turnover/income] AND [staff/staff or volunteers] TEXT SUBSTITUTIONS ON TYPEXDUM (USE CHARITY TEXT IF TYPEXDUM CODE 2, ELSE BUSINESS TEXT)

ASK IF NOT SKIPPING QUESTIONS (CONSENTCDUM NOT CODE 1)
**Q2.SIZEA**
ASK IF NOT CHARITY OR PUBLIC SECTOR (TYPEXDUM CODES 1, 4 OR 5): Including yourself, how many employees work in your organisation across the UK as a whole?
ADD IF NECESSARY: By that I mean both full-time and part-time employees on your payroll, as well as any working proprietors or owners in the UK.
ASK IF CHARITY (TYPEXDUM CODE 2): Including yourself, how many employees, volunteers and trustees working in your organisation across the UK as a whole?
ADD IF NECESSARY: By that I mean both full-time and part-time employees on your payroll, as well as people who regularly volunteer for your organisation in the UK. This does not include operations outside the UK.
ASK IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEXDUM CODE 3): Including yourself, how many employees and council members are there in your organisation?
ASK IF OTHER PUBLIC SECTOR (SAMPLE S_LASTATUS≠1 OR 2 AND TYPEXDUM CODE 3): Including yourself, how many employees work in your organisation? For example, if you were working in an NHS Trust, we want to know how many people work in that Trust, not the NHS as a whole.
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE 2 TO 99,999
(SOFT CHECK IF >9,999)
DO NOT READ OUT: Don’t know
Respondent is sole trader CLOSE SURVEY IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)

ASK IF DON’T KNOW SIZE OF ORGANISATION (SIZEA CODE DK)
**Q3.SIZEB**
ASK IF NOT CHARITY OR PUBLIC SECTOR (TYPEXDUM CODES 1, 4 OR 5): Which of these best represents the number of employees working in your organisation across the UK as a whole, including yourself?
ASK IF CHARITY (TYPEXDUM CODE 2): Which of these best represents the number of employees, volunteers and trustees working in your organisation across the UK as a whole, including yourself?
ASK IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEXDUM CODE 3): Which of these best represents the number of employees and council members in your organisation, including yourself?
ASK IF OTHER PUBLIC SECTOR (SAMPLE S_LASTATUS≠1 OR 2 AND TYPEXDUM CODE 3): Which of these best represents the number of employees working in your organisation across the UK as a whole, including yourself?
PROBE FULLY, I.E. UNTIL YOU REACH THE RIGHT RESPONSE

SINGLE CODE
Under 10
10 to 49
50 to 249
250 to 999
1,000 or more
DO NOT READ OUT: Don’t know

DUMMY VARIABLE NOT ASKED
**Q3a.SIZE**
Which of these best represents the number of employees, volunteers and trustees working in your organisation, including yourself?

SINGLE CODE, MERGE RESPONSES FROM SAMPLE S_SECTORALSIZE, SIZEA AND SIZEB
Under 10
10 to 49
50 to 249
250 to 999
1,000 or more

Don’t know

ASK IF IDBR SAMPLE BUT SELF-IDENTIFY AS CHARITY IN QUESTIONNAIRE (SAMPLE S_TYPE=1 AND TYPEXDUM CODE 2)
**Q4.SALESA**
In the financial year just gone, what was the approximate income of your organisation across the UK as a whole?
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE £0+
(SOFT CHECK IF <£1,000 OR >£50,000,000)
DO NOT READ OUT: Don’t know
DO NOT READ OUT: Refused

ASK IF DON’T KNOW NUMERIC TURNOVER OF ORGANISATION (SALESA CODE DK OR REF)
**Q5.SALESB**
Which of these best represents the income of your organisation across the UK as a whole in the financial year just gone?
PROBE FULLY, I.E. UNTIL YOU REACH THE RIGHT RESPONSE

SINGLE CODE
£0 to under £10,000
£10,000 to under £100,000
£100,000 to under £500,000
£500,000 to under £5 million
£5 million or more
DO NOT READ OUT: Don’t know
DO NOT READ OUT: Refused

DUMMY VARIABLE NOT ASKED
**Q5a.SALES**
Which of these best represents the income of your organisation across the UK as a whole in the financial year just gone?

SINGLE CODE, MERGE RESPONSES FROM SAMPLE S_INCOMEBAND, SALESA AND SALESB
£0 to under £10,000
£10,000 to under £100,000
£100,000 to under £500,000
£500,000 to under £5 million
£5 million or more
Don’t know
Refused

**Q6.DEFINE DELETED POST-PILOT IN 2018**

## Outsourcing

ASK IF NOT CYBER SECTOR (TYPXDUM NOT CODE 4)
**Q7.OUTSOURCE**
Are any aspects of your cyber security handled by individuals or organisations outside your own organisation? This does **not** include software firms providing technical support or security updates for their own applications, such as Microsoft updates to Office 365.
ADD IF NECESSARY: This may include a service provider that manages your IT or network, or helps you recover from cyber incidents.
DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

READ OUT IF OUTSOURCE (OUTSOURCE CODE 1)
I’d now like to ask a few more questions about this outsourcing.

**Q8.HOWMUCH DELETED IN 2020**

**Q9.REASONOUT DELETED IN 2020**

**Q10.INVESTOUT DELETED POST-PILOT IN 2018**

**Q11.INVESTOUTB DELETED POST-PILOT IN 2018**

**Q12.OUTVALUES DELETED POST-PILOT IN 2018**

ASK IF OUTSOURCE (OUTSOURCE CODE 1)
**Q13.WHATOUT**
Which of the following aspects of cyber security are covered by your outsourced provider or providers?
READ OUT

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP i LAST

a. Setting up firewalls
b. Choosing secure settings for devices or software
c. Controlling which users have IT or admin rights
d. Detecting and removing malware on the organisation's devices
e. Keeping software up to date
f. Restricting what software can run on the organisation's devices
g. Creating back-ups of your files and data
h. Incident response or recovery
i. Any higher-level functions, which could include things like:
   - security engineering or architecture
   - penetration testing
   - using threat intelligence tools
   - forensic analysis
   - interpreting malicious code
   - or using tools to monitor user activity
j. An external Security Operations Centre

SINGLE CODE
Yes, outsourced
No, not outsourced
DO NOT READ OUT: Don't know

ASK IF OUTSOURCE HIGHER-LEVEL FUNCTIONS (WHATOUTi CODE 1)
**Q14.WHATHIGHER**
Which of the following specific higher-level functions are covered by your outsourced provider or providers?
READ OUT

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP g LAST

a. Designing secure networks, systems and application architectures
b. Penetration testing
c. Using cyber threat intelligence tools or platforms
d. Carrying out forensic analysis of cyber security breaches
e. Interpreting malicious code, or the results shown after running anti-virus software
f. Using tools to monitor user activity

SINGLE CODE
Yes
No
DO NOT READ OUT: Don't know

**Q15.DEALINGOUT DELETED IN 2020**

**Q16.PERFORMOUT DELETED POST-PILOT IN 2018**

## Workforce size

READ OUT IF NOT CYBER SECTOR (TYPXDUM NOT CODE 4)
Now I'd like to ask some questions about you and others **within** your organisation.

**Q16a.TITLE DELETED IN 2021**

ASK IF NOT CYBER SECTOR (TYPXDUM NOT CODE 4)
**Q17.TEAM**
Within your organisation, how many people, including yourself, are directly involved in managing or running your organisation's cyber security? [IF OUTSOURCE (OUTSOURCE CODE 1): This includes whoever deals with your outsourced provider.]

WRITE IN RANGE 1 TO [SIZEA OR TOP END OF SIZEB] OR [99 IF SIZE=DK]
IF MICRO (SIZEA CODE<10 OR SIZEB CODE 1): (SOFT CHECK IF >3)
IF SMALL (SIZEA 9<CODE<50 OR SIZEB CODE 2): (SOFT CHECK IF >9)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF >9)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4 TO 5 OR DK]): (SOFT CHECK IF >30)
DO NOT READ OUT: Don't know

ASK IF CYBER SECTOR, NOT SOLE TRADER AND NOT SKIPPING QUESTIONS (SIZEA NOT SOLE TRADER CODE AND CONSENTCDUM CODE 2)
**Q17a.CYBERSIZE**
How many of your VALUE AT SIZEA OR SIZEB EXCEPT IF SIZEB CODE DK employees are **working in cyber security roles**? By that we mean anyone involved in the development, sales or delivery of cyber security products or services.
PROBE FOR BEST ESTIMATE BEFORE CODING DON'T KNOW

WRITE IN RANGE 1 TO SIZEA OR TOP END OF SIZEB, OTHERWISE 99,999
(SOFT CHECK IF >9,999)
DO NOT READ OUT: Don't know

ASK IF DON'T KNOW EXACT NUMBER OF CYBER STAFF (CYBERSIZE CODE DK)
**Q17b.CYBERSIZEB**
Are there approximately … ?
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)

SINGLE CODE AND ONLY SHOW CODES AT OR UNDER CODE AT SIZEA OR SIZEB
1 to 4
5 to 9
10 to 29
30 to 49
50 to 249
250 to 499
500 to 999
1,000 or more
DO NOT READ OUT: Don't know

DUMMY VARIABLE NOT ASKED
**Q17c.CYBERSIZEDUM**
How many of your employees are working in cyber security roles?

MERGE RESPONSES FROM SAMPLE S_SECTORALCYBERSIZE AND CYBERSIZE, AND SIZEA IF SOLE TRADER
WRITE IN RANGE 1 TO 99,999
Don't know

DUMMY VARIABLE NOT ASKED
**Q17d.CYBERSIZEBDUM**
How many of your employees are working in cyber security roles?

SINGLE CODE, MERGE RESPONSES FROM SAMPLE S_SECTORALCYBERSIZE, S_SECTORALCYBERSIZEB, CYBERSIZE AND CYBERSIZEB, AND SIZEA IF SOLE TRADER

1 to 4
5 to 9
10 to 29
30 to 49
50 to 249
250 to 499
500 to 999
1,000 or more
Don’t know

ASK IF NOT CYBER SECTOR (TYPXDUM NOT CODE 4)
**Q18.PATHWAY**
ASK IF ONE PERSON (TEAM=1): How did you enter this role dealing with cyber security within your organisation?
ASK IF MORE THAN ONE PERSON (TEAM>1 OR DK): Of all the [TEAM] people directly involved in cyber security within your organisation, how many entered this role in each of the following ways?
READ OUT
IF ONE PERSON (TEAM=1): INTERVIEWER NOTE: CODE “1” AT RELEVANT RESPONSE

ASK AS A GRID

a. Absorbing this role into an ongoing **non**-cyber security related role
b. Recruited **internally** into a cyber-specific role
c. Recruited **externally** from a **non**-cyber security related previous role
d. Recruited **externally** from a previous role in cyber security
e. As a career starter, for example a graduate or apprentice

WRITE IN RANGE 1 TO TEAM OR [99 IF TEAM=DK] FOR EACH STATEMENT
HARD CHECK IF TOTAL ACROSS STATEMENTS >TEAM
DO NOT READ OUT: Don’t know

READ OUT IF CYBER SECTOR AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1)
Now I would like to ask some questions about the people working in cyber security roles **within** your organisation, including you.
IF SKIPPING QUESTIONS (CONSENTCDUM CODE 1): In the previous survey you took part in, we recorded that this was [CYBERSIZEDUM OR CYBERSIZEBDUM] employees.

ASK IF CYBER SECTOR AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1)
**Q18a.CYBERSENIOR**
Of all these [CYBERSIZEDUM OR CYBERSIZEBDUM] employees, how many are principal or director-level staff? These staff typically have around 6 or more years of experience.

WRITE IN RANGE 1 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM FOR EACH STATEMENT
HARD CHECK IF TOTAL ACROSS STATEMENTS >CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM
DO NOT READ OUT: Don’t know

DUMMY VARIABLE NOT ASKED
**Q18x.CYBERSENIORDUM**
How many are principal or director-level staff?

SINGLE CODE
IF CYBERSIZEDUM=1, CODE 1
OTHERWISE MERGE RESPONSES FROM CYBERSENIOR

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
**Q18b.PATHWAYNUM**
IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Did you enter this role in any of the following ways?
IF MORE THAN ONE (CYBERSIZEDUM≠1): Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, including you, how many entered this role in each of the following ways?
READ OUT

ASK AS A GRID

a. Recruited or joined from a **non**-cyber security related previous role
b. Recruited or joined from a previous role in cyber security
c. As a career starter, for example a graduate or apprentice

WRITE IN RANGE 1 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM FOR EACH STATEMENT
HARD CHECK IF TOTAL ACROSS STATEMENTS >CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM
DO NOT READ OUT: Don't know

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4 TO DK)
**Q18c.PATHWAYPER**
Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, including you, roughly what percentage entered this role in each of the following ways?
READ OUT
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)

ASK AS A GRID

a. Recruited or joined from a **non**-cyber security related previous role
b. Recruited or joined from a previous role in cyber security
c. As a career starter, for example a graduate or apprentice

SINGLE CODE
None of them
Under a quarter
More than a quarter, under a half
More than a half, under three-quarters
More than three-quarters, but not all
All of them (i.e. 100%)
DO NOT READ OUT: Don't know

## Workforce diversity

**Q19.DIVERSITYA DELETED IN 2020**

READ OUT IF CYBER SECTOR (TYPEXDUM CODE 4)
These next questions help the government to measure diversity across the whole cyber security sector. The answers won't be linked to your business.

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
**Q19a.FEMALENUM**
Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, how many are female?
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

WRITE IN RANGE 0 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
**Q19b.BAMENUM**
How many are from ethnic minority backgrounds?
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

WRITE IN RANGE 0 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
**Q19x.DISABILITYNUM**
How many have a disability? That is, any long-standing illness, condition or impairment, which causes difficulty with day-to-day activities.
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

WRITE IN RANGE 0 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM

DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
**Q19c.NEURONUM**
How many have neurodiverse conditions or learning disorders, such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD)?
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

WRITE IN RANGE 0 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

**Q20.DIVERSITYB DELETED IN 2020**

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4 TO DK)
**Q20a.FEMALEPER**
Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, roughly what percentage are female?
PROBE FOR BEST ESTIMATE BEFORE CODING DON'T KNOW
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

WRITE IN RANGE 0 TO 100
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF CAN'T SAY EXACT PERCENTAGE (FEMALEPER CODE DK OR REF)
**Q20b.FEMALEPERB**
Is it … ?
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)

SINGLE CODE
None of them
Under a quarter
More than a quarter, under a half
More than a half, under three-quarters
More than three-quarters, but not all
All of them (i.e. 100%)
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF LARGE CYBER SECTOR (TYPXDUM CODE 4 AND CYBERSIZEBDUM CODES 4 TO DK)
**Q20c.BAMEPER**
Roughly what proportion are from ethnic minority backgrounds?
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

SINGLE CODE
None of them
Under a quarter
More than a quarter, under a half
More than a half, under three-quarters
More than three-quarters, but not all
All of them (i.e. 100%)
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4 TO DK)
**Q20d.DISABILITYPER**

Roughly what proportion have a disability? That is, any long-standing illness, condition or impairment, which causes difficulty with day-to-day activities.
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

SINGLE CODE
None of them
Under a quarter
More than a quarter, under a half
More than a half, under three-quarters
More than three-quarters, but not all
All of them (i.e. 100%)
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4 TO DK)
**Q20e.NEUROPER**
Roughly what proportion have neurodiverse conditions or learning disorders, such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD)?
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

SINGLE CODE
None of them
Under a quarter
More than a quarter, under a half
More than a half, under three-quarters
More than three-quarters, but not all
All of them (i.e. 100%)
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF HAVE WOMEN IN CYBER ROLES ((FEMALENUM>0 AND NOT REF) OR (FEMALEPER>1 OR REF) OR (FEMALEPERB NOT CODE 1 OR REF))
**Q20xb.FEMALESENIOR**
How many of the female employees in these roles are principal or director-level staff? These staff typically have around 6 or more years of experience.
ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

WRITE IN RANGE 0 TO LOWEST OF FEMALENUM, CYBERSIZEDUM, TOP OF CYBERSIZEBDUM OR 99
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF HAVE ETHNIC MINORITIES IN CYBER ROLES (BAMENUM>0 AND NOT REF) OR (BAMEPER>1 OR REF) OR (BAMEPERB NOT CODE 1 OR REF))
**Q20xc.BAMESENIOR**
How many of the ethnic minority employees in these roles are principal or director-level staff? These staff typically have around 6 or more years of experience.
ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

WRITE IN RANGE 0 TO LOWEST OF BAMENUM, CYBERSIZEDUM, TOP OF CYBERSIZEBDUM OR 99
DO NOT READ OUT: Don't know
DO NOT READ OUT: Prefer not to say

ASK IF HAVE DISABLED PEOPLE IN CYBER ROLES (DISABILITYNUM>0 AND NOT REF) OR (DISABLITYPER>1 OR REF) OR (DISABLITYPERB NOT CODE 1 OR REF))
**Q20xd.DISABILITYSENIOR**
How many of the disabled people in these roles are principal or director-level staff? These staff typically have around 6 or more years of experience.
ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

WRITE IN RANGE 0 TO LOWEST OF DISABLILTYNUM, CYBERSIZEDUM, TOP OF CYBERSIZEBDUM OR 99

DO NOT READ OUT: Don’t know
DO NOT READ OUT: Prefer not to say

ASK IF HAVE NEURODIVERGENT PEOPLE IN CYBER ROLES (NEURONUM>0 AND NOT REF) OR (NEUROPER>1 OR REF) OR (NEUROPERB NOT CODE 1 OR REF))

**Q20xe.NEUROSENIOR**
How many of the people with neurodiverse conditions in these roles are principal or director-level staff? These staff typically have around 6 or more years of experience.
ADD IF NECESSARY: We’d like an approximate number rather than a percentage.

WRITE IN RANGE 0 TO LOWEST OF DISABLILTYNUM, CYBERSIZEDUM, TOP OF CYBERSIZEBDUM OR 99
DO NOT READ OUT: Don’t know
DO NOT READ OUT: Prefer not to say

**Q21.DIVERSITYDUM DELETED IN 2020**

## Workforce qualifications

ASK IF CYBER SECTOR (TYPEXDUM CODE 4)

**Q22.QUALS**
Do you or any other employees in cyber security roles have, or are they working towards, any cyber security-related qualifications or certified training?
DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

ASK IF QUALIFICATIONS (QUALS CODE 1)

**Q23.WHICHQUALS**
Which of the following types of qualifications or certified training do you or other employees have, or are they working towards?
READ OUT

MULTICODE
A specialist higher education qualification (e.g. a degree) related to cyber security
A general computer science, information systems or IT higher education qualification
A cyber security apprenticeship
Any other apprenticeship
Any other technical qualifications or certified training related to cyber security
SINGLE CODE
DO NOT READ OUT: Don’t know
DO NOT READ OUT: None of these

**Q24.WHICHCERT DELETED IN 2021**

**Q25.SENIORITY DELETED IN 2020**

## Formal versus informal cyber security roles

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)

**Q26.FORMAL**
Is cyber security a formal part of your job description, or do you cover this role informally?
DO NOT READ OUT

SINGLE CODE
A formal part of their job description
Covered informally
Don’t know

**Q27.COVER DELETED IN 2021**

## Skills and knowledge of responsible individual or team

ASK ALL
**Q28.RELATIVE**
How important would you say it is for all the employees in cyber security roles within your organisation to possess each of the following? Please answer on a scale of 0 to 10, where 0 means not at all important and 10 means essential.
READ OUT

RANDOMISE STATEMENT ORDER BUT KEEP f AND g TOGETHER

a. IF CYBER SECTOR (TYPEXDUM CODE 4): Soft skills, such as oral or written communication skills and team working skills
b. **STATEMENT DELETED POST-PILOT IN 2018**
c. **STATEMENT DELETED IN 2020**
d. IF CYBER SECTOR (TYPEXDUM CODE 4): Understanding the legal or compliance issues affecting cyber security, such as data protection
e. **STATEMENT DELETED IN 2020**
f. **STATEMENT DELETED IN 2021**
g. IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4): **High-level technical skills**, which could include things like:
   - security engineering or architecture
   - penetration testing
   - using threat intelligence tools
   - forensic analysis
   - interpreting malicious code
   - or using tools to monitor user activity
h. IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4): **Incident response skills**, which could include things like writing an incident response plan, incident management and recovery from cyber security breaches

WRITE IN RANGE 0 TO 10
DO NOT READ OUT: Don’t know

SCRIPT TO ROTATE ORDER OF TECHNICAL, MANAGERIAL AND KNOWLEDGE

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
**Q29.TECHNICAL**
How confident, if at all, would you feel about [IF MORE THAN ONE PERSON (TEAM>1 OR DK): you or any of the other individuals directly involved in cyber security] being able to do each of the following **technical** tasks in your work?
ADD IF NECESSARY: If you don’t currently need to do this in your work, we’d like to know how confident, if at all, you would feel about being able to do it in the future.
READ OUT

RANDOMISE STATEMENT ORDER

a. Storing or transferring personal data securely, using encryption where appropriate
b. ASK IF NOT OUTSOURCED (WHATOUTa NOT CODE 1): Setting up firewalls with appropriate configurations
c. ASK IF NOT OUTSOURCED (WHATOUTb NOT CODE 1): Choosing secure settings for devices or software
d. ASK IF NOT OUTSOURCED (WHATOUTc NOT CODE 1): Controlling which users have IT or admin rights
e. ASK IF NOT OUTSOURCED (WHATOUTd NOT CODE 1): Detecting and removing malware on the organisation's devices
f. ASK IF NOT OUTSOURCED (WHATOUTe NOT CODE 1): Setting up software to automatically update where possible
g. ASK IF NOT OUTSOURCED (WHATOUTf NOT CODE 1): Restricting what software can run on the organisation's devices
h. ASK IF NOT OUTSOURCED (WHATOUTg NOT CODE 1): Creating back-ups of your files and data
i. ASK IF NOT OUTSOURCED (WHATOUTh NOT CODE 1): Dealing with a cyber security breach or attack
j. ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEg>4 AND WHATHIGHERa NOT CODE 1): Designing secure networks, systems and application architectures
k. ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEg>4 AND WHATHIGHERb NOT CODE 1): Carrying out a penetration test

l. ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEg>4 AND WHATHIGHERc NOT CODE 1): Using cyber threat intelligence tools or platforms
m. ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEg>4 AND WHATHIGHERd NOT CODE 1): Carrying out a forensic analysis of a cyber security breach
n. ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEg>4 AND WHATHIGHERe NOT CODE 1): Interpreting malicious code, or the results shown after running anti-virus software
o. ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEg>4 AND WHATHIGHERf NOT CODE 1): Using tools to monitor user activity

SINGLE CODE, ALLOW REVERSED SCALE
Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don’t know

READ OUT IF CYBER SECTOR (TYPEXDUM CODE 4):
These next questions are about performing tasks for your organisation’s **own** cyber security, not that of any customers.

ASK ALL
**Q30.MANAGERIAL**
IF CYBER SECTOR (TYPEXDUM CODE 4):
How confident, if at all, would you feel about your organisation being able to perform the following tasks, given the current skill levels of your workforce?

IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4):
How confident, if at all, would you feel about [IF MORE THAN ONE PERSON (TEAM>1 OR DK): you or any of the other individuals directly involved in cyber security] being able to do each of the following **communication or managerial** tasks in your work?
ADD IF NECESSARY: If you don’t currently need to do this in your work, we’d like to know how confident, if at all, you would feel about being able to do it in the future.
READ OUT

RANDOMISE STATEMENT ORDER
a. ASK HALF THE SAMPLE (HALF A): Communicating cyber security risks effectively to directors, trustees or senior management
b. ASK HALF THE SAMPLE (HALF B): Giving guidance to other staff on what an acceptably strong password is
c. ASK HALF THE SAMPLE (HALF A): Writing an incident response plan to deal with cyber security breaches
d. ASK HALF THE SAMPLE (HALF B): Carrying out a cyber security risk assessment
e. ASK HALF THE SAMPLE (HALF A): Carrying out a data protection impact assessment
f. ASK HALF THE SAMPLE (HALF B): Writing or contributing to a business continuity plan that covers cyber security
g. ASK HALF THE SAMPLE (HALF A): Preparing training materials or training sessions for staff who are not specialists in cyber security
h. **STATEMENT DELETED POST-PILOT IN 2018**
i. ASK HALF THE SAMPLE (HALF B): Developing cyber security policies

SINGLE CODE, ALLOW REVERSED SCALE
Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don’t know

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
**Q31.KNOWLEDGE**
How well, if at all, would you say you [IF MORE THAN ONE PERSON (TEAM>1 OR DK): or any of the other individuals directly involved in cyber security] understand each of the following?
READ OUT

RANDOMISE STATEMENT ORDER

a. ASK HALF THE SAMPLE (HALF A): The difference between a personal and a boundary firewall
b. ASK HALF THE SAMPLE (HALF B): What a sandboxed application is
c. ASK HALF THE SAMPLE (HALF A): Your organisation's data protection requirements
d. ASK HALF THE SAMPLE (HALF B): How any actions or policies around cyber security can affect the organisation’s performance and success
e. **STATEMENT DELETED POST-PILOT IN 2018**
f. **STATEMENT DELETED POST-PILOT IN 2018**

SINGLE CODE, ALLOW REVERSED SCALE
Very well
Fairly well
Not very well
Not at all well
DO NOT READ OUT: Don’t know

## Skills and knowledge of wider staff (non-cyber firms)

READ OUT IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
The next questions are about the current skills and knowledge of wider [staff/staff and volunteers], beyond those who are directly involved in cyber security.

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
**Q32.DIRECTORS**
How well, if at all, would you say your organisation’s [directors/trustees] or senior managers [IF LOWER-TIER LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 AND TYPEX CODE 4):, including council members,] understand each of the following?
READ OUT

RANDOMISE STATEMENT ORDER

a. The cyber security risks facing your organisation
b. Your organisation's data protection requirements
c. When cyber security breaches need to be reported externally, for example to a regulator
d. The steps that need to be taken when managing a cyber security incident
e. **STATEMENT DELETED POST-PILOT IN 2018**
f. **STATEMENT DELETED POST-PILOT IN 2018**
g. **STATEMENT DELETED POST-PILOT IN 2018**
h. The staffing needs of cyber security within your organisation

SINGLE CODE, ALLOW REVERSED SCALE
Very well
Fairly well
Not very well
Not at all well
DO NOT READ OUT: Don’t know

**Q33.DIRECTDUM DELETED IN 2020**

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
**Q34.CORE**
How confident, if at all, would you feel in your organisation’s core [staff/staff or volunteers] [IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEX CODE 4): or council members] as a whole being able to do each of the following?
READ OUT

RANDOMISE STATEMENT ORDER

**a. STATEMENT DELETED POST-PILOT IN 2018**
b. Store or transfer personal data securely, using encryption where appropriate
c. Use acceptably strong passwords
d. Detect malware on the organisation's devices
e. Identify fraudulent emails or fraudulent websites
f. Work collaboratively with those directly responsible for dealing with cyber security breaches

SINGLE CODE, ALLOW REVERSED SCALE
Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don’t know

## Training and upskilling

READ OUT IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
Now I’d like to ask about formal training and awareness raising activities around cyber security. This is for both people working in cyber security roles and wider staff.

READ OUT IF CYBER SECTOR (TYPEXDUM CODE 4)
Now I’d like to ask about formal training and upskilling around cyber security.

**Q35.VALUE DELETED POST-PILOT IN 2018**

ASK ALL
**Q35a.NEEDSAWARE**
How well, if at all, would you say you understand the kinds of cyber security training and skills people in your organisation need?
READ OUT

SINGLE CODE, ALLOW REVERSED SCALE
Very well
Fairly well
Not very well
Not at all well
DO NOT READ OUT: Don’t know

ASK ALL
**Q36.NEEDS**
In the last 12 months, has anyone undertaken a formal analysis of your organisation’s cyber security skills or training needs?
DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

SCRIPT TO ASK TRAINED TO WORTH AS A LOOP FOR EACH OF THE FOLLOWING AUDIENCES:

a. you [IF MORE THAN ONE PERSON (TEAM>1 OR DK OR CYBERSIZEDUM≠1): or any of the other employees in cyber security roles]
b. ASK IF NOT A LOWER-TIER LOCAL AUTHORITY AND NOT CYBER SECTOR (SAMPLE S_LASTATUS≠1 AND TYPEXDUM NOT CODE 4): any other [staff/staff or volunteers] [IF HIGHER-TIER LOCAL AUTHORITY (SAMPLE S_LASTATUS=2 AND TYPEX CODE 4): or council members] who are not directly involved in cyber security

**QSOUGHT DELETED IN 2020**

ASK AS PART OF TRAINED TO WORTH LOOP
**Q37a.TRAINED**
In the last 12 months, have you carried out any cyber security training [IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4): or awareness raising sessions] specifically for [SCRIPT TO ADD LOOP TEXT]?
DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

ASK AS PART OF TRAINED TO WORTH LOOP IF CARRIED OUT TRAINING (TRAINED CODE 1)
**Q37b.FORMAT**
Was any of the training for this group … ?
READ OUT STATEMENTS

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP a AND b TOGETHER

a. IF LOOP A: Introductory training for new joiners or graduates entering cyber security roles
b. IF LOOP A: Continuing professional development training for staff who are not new joiners
c. IF LOOP B: **Specific** training sessions devoted to cyber security
d. **STATEMENT DELETED IN 2021**
e. **STATEMENT DELETED IN 2021**
f. Developed internally within the organisation
g. Delivered internally within the organisation
h. Developed externally outside the organisation
i. Delivered externally outside the organisation
j. Mandatory training
k. IF LOOP B: Specifically covering home working or use of personal devices

SINGLE CODE
Yes
No
Don’t know

**Q38.BARRIERS DELETED IN 2020**

**Q39.MODE DELETED IN 2020**

**Q40.TRAINER DELETED POST-PILOT IN 2018**

**Q41.TRAINERDUM DELETED POST-PILOT IN 2018**

ASK AS PART OF TRAINED TO WORTH LOOP IF CARRIED OUT TRAINING (TRAINED CODE 1)
**Q42.WORTH**
How much would you say the current programme of training you have for this group of staff has met your overall training and skills needs?
ADD IF NECESSARY: We are talking about [SCRIPT TO ADD LOOP TEXT].
READ OUT

SINGLE CODE, ALLOW REVERSED SCALE
Completely
A great deal
A fair amount
Not very much
Not at all
DO NOT READ OUT: Don’t know

## Recruitment

READ OUT IF CYBER SECTOR (TYPEXDUM CODE 4)
I’d now like to ask about recruitment in cyber security job roles.

ASK IF CYBER SECTOR (TYPEXDUM CODE 4)
**Q43.RECRUIT**
Since the start of 2019, have you tried to recruit anyone to fill any cyber skills needs in your organisation? This includes any current vacancies you may have.
DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
**Q44.OTHRECRUIT**
What recruitment methods have you used to find candidates for these vacancies?
DO NOT READ OUT
PROBE FULLY, I.E. “ANYTHING ELSE?”
INTERVIEWER NOTE: IF RECRUITMENT AGENCY OR WEBSITE, WERE THESE SPECIALIST AGENCIES/WEBSITES FOR CYBER SECURITY OR GENERALIST?

MULTICODE RESPONSES UNDER THE BOLD HEADINGS
**Recruitment agencies**
Generalist recruitment agency
Specialist cyber security recruitment agency

**Online/recruitment websites**
Job ads on our own website
Generalist recruitment website, e.g. Indeed
Specialist cyber security recruitment website, e.g. Cybersecurityjobsite.com
Posts or ads on social networks like Facebook, Twitter or LinkedIn
Online ads outside social networks

**Other**
Ads in newspapers or magazines
Asking individuals to apply directly
Graduate schemes
Headhunting (but not through recruitment agency)
Partnering with schools/colleges
Partnering with universities
Recruiting from elsewhere in organisation
Word-of-mouth/industry networks/recommendations
Other WRITE IN

SINGLE CODE
Don’t know

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
**Q45.VACANCIES**
Since the start of 2019, how many vacancies have you had in cyber security roles?
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE 1 TO 99
IF MICRO (SIZEA CODE<10 OR SIZEB CODE 1): (SOFT CHECK IF >3)
IF SMALL (SIZEA 9<CODE<50 OR SIZEB CODE 2): (SOFT CHECK IF >9)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF >9)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4 TO 5 OR DK]): (SOFT CHECK IF >30)
DO NOT READ OUT: Don’t know

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
**Q46.HARD**
IF ONE VACANCY (VACANCIES=1): And has this vacancy proved hard to fill for any reason? This is even if you have since filled this vacancy.
IF MORE THAN ONE VACANCY (VACANCIES>1 OR DK): And how many vacancies, if any, have proved hard to fill for any reason? This includes vacancies that you may have since filled.
IF ONE VACANCY (VACANCIES=1): INTERVIEWER NOTE: CODE “1” IF HARD-TO-FILL, OTHERWISE 0
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE 0 TO VACANCIES OR [(SIZEA OR TOP END OF SIZEB) IF VACANCIES=DK] OR [99 IF SIZE=DK]
DO NOT READ OUT: Don’t know

ASK IF HARD-TO-RECRUIT VACANCIES (HARD>0)
**Q46b.HARDROLE**
IF ONE VACANCY (VACANCIES=1): What specific role or occupation was this hard-to-fill vacancy in?

IF MORE THAN ONE VACANCY (VACANCIES>1 OR DK): What specific roles or occupations were these hard-to-fill vacancies in?
PROMPT TO CODE
READ OUT TEXT IN BOLD BEFORE CODING "OTHER". ADD ADDITIONAL DESCRIPTIONS IF NECESSARY.
INTERVIEWER NOTE: IF JUST "ANALYST" OR "CONSULTANT", PROMPT WITH BOLD TEXT BEFORE CODING "OTHER".

MULTICODE RESPONSES UNDER THE UNDERLINED HEADINGS UP TO HARD
Generalist roles
**Generalist cyber security role**
**Generalist IT role**
**Generalist sales role**

Specialist roles
**Senior management role**, e.g. a Chief Information Security Officer (CISO), Head of Information Security or Head of Cyber Security
**Risk management role**, e.g. a Information Security Risk Manager/Officer
**Security management role**, e.g. a System Security Manager/Officer ensuring that security controls are in place and operating as designed
**Communications security role**, e.g. a ComSec Manager/Officer, managing the security of emails or cryptographic systems
**Security Architect**, developing and reviewing an organisation's security architecture
**Penetration Tester**, analysing and testing the security of infrastructures, systems, websites and apps
**Threat Analyst**, analysing intelligence to identify, monitor, assess and counter cyber threats
**Vulnerability Assessment Analyst**, analysing and testing the security of infrastructures, systems, websites and apps
Other WRITE IN
SINGLE CODE
DO NOT READ OUT: Don't know

ASK IF HARD-TO-RECRUIT VACANCIES (HARD>0)
**Q46c.HARDSENIOR**
IF ONE VACANCY (VACANCIES=1): What level of seniority was this hard-to-fill vacancy?
IF MORE THAN ONE VACANCY (VACANCIES>1 OR DK): What levels of seniority were these hard-to-fill vacancies?
PROMPT TO CODE

MULTICODE UP TO HARD
Apprentices
Entry-level staff or graduates
Experienced or senior staff, typically with around 3 to 5 years of experience
Principal-level staff, typically with around 6 to 9 years of experience
Director-level, typically with around 10 or more years of experience
SINGLE CODE
DO NOT READ OUT: Don't know

ASK IF HARD-TO-RECRUIT VACANCIES (HARD>0)
**Q47.HARDREASON**
IF ONE VACANCY (VACANCIES=1): What are the reasons this vacancy has been hard to fill?
IF MORE THAN ONE VACANCY (VACANCIES>1 OR DK): What are the reasons these vacancies have been hard to fill?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"

MULTICODE RESPONSES UNDER THE BOLD HEADINGS
**Offer not good enough**
Job is difficult/challenging
Low pay or benefits/salary demand too high
Not offering training
Poor career progression/lack of prospects
Too much competition from other employers

**Quality of candidates**

Lack of candidates with the required attitude, motivation or personality
Lack of soft skills, e.g. communication skills
Lack of technical skills/knowledge
Lack of qualifications
Lack of work experience

**Other reasons**
Cultural fit/not matching our culture
Lack of candidates generally
Recruitment budget cuts
Remote location/poor public transport
Other WRITE IN

SINGLE CODE
Don't know

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
**Q47a.DIVERSERECRUIT**
In the last 18 months, has your organisation changed or adapted your recruitment processes, or carried out any specific activities to encourage applications from the following groups of people?
READ OUT STATEMENTS

ASK AS A GRID

a. Women
b. People from ethnic minority backgrounds
c. Disabled people
d. People with neurodiverse conditions or learning disorders, such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD)?

SINGLE CODE
Yes
No
Don't know

ASK IF CYBER SECTOR (TYPEXDUM CODE 4)
**Q47b.INTERN**
Since the start of 2019, have you offered any internships or work placements in cyber security roles?
DO NOT READ OUT

SINGLE CODE
Yes
No
Don't know

## Staff turnover

READ OUT IF CYBER SECTOR (TYPEXDUM CODE 4)
Finally, I'd like to ask about the staff turnover in cyber security job roles.

ASK IF CYBER SECTOR (TYPEXDUM CODE 4)
**Q47x.LEFT**
In the last 18 months, have any employees in cyber security roles left your company or retired?
DO NOT READ OUT

SINGLE CODE
Yes
No
Don't know

ASK LEFTA AND LEFTB AS A LOOP FOR EACH STATEMENT AT RETIREA

ASK IF EMPLOYEES HAVE LEFT (LEFT CODE 1)
**Q47c.LEFTA**

In the last 18 months, how many employees in cyber security roles, if any, have left your company for each of the following reasons?
READ OUT

ASK AS A GRID

a. Retirement
b. Dismissal
c. Redundancy as a result of COVID-19
d. Redundancy **not** as a result of COVID-19
e. Of their own volition

WRITE IN RANGE 0 TO 49 FOR EACH STATEMENT
IF MICRO/SMALL (SIZEA CODE<50 OR (SIZEB CODES 1 TO 2)): (SOFT CHECK IF >3)
IF MEDIUM/LARGE (SIZEA 49<CODE OR (SIZEB CODES 3 TO 5 OR DK): (SOFT CHECK IF >19)
DO NOT READ OUT: Don't know

ASK FOR EACH STATEMENT IF DON'T KNOW HOW MANY HAVE LEFT (LEFTAa-e CODE DK)
**Q47d.LEFTB**
Was it … ?
PROBE FULLY, I.E. UNTIL YOU REACH THE RIGHT RESPONSE

SINGLE CODE
None
1 to 2
3 to 4
5 to 9
10 to 14
15 to 19
20 to 24
25 to 29
More than 30
DO NOT READ OUT: Don't know

ASK IF HAD EMPLOYEES THAT LEFT OF THEIR OWN VOLITION (LEFTAe>0 OR LEFTBe CODES 2-9)
**Q47e.REASON**
As far as you know, what reasons did employees have for leaving of their own volition?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"

MULTICODE RESPONSES UNDER THE BOLD HEADINGS
**Company offer not good enough**
Better pay or benefits elsewhere
Lack of career development opportunities
Lack of training
Offered more senior position elsewhere

**Other reasons**
Company culture
Changed career/left cyber security
Change in personal circumstances
Job too difficult/challenging
Relationship with line manager
Remote location/poor public transport
Stress/overworked
Work-life balance
Other WRITE IN

SINGLE CODE
Don't know

## Recontact

ASK ALL

**Q48.RECON**
Would you be happy to take part in a more bespoke interview with Ipsos MORI in autumn 2020, to further explore some of the issues from this survey? This interview would be more of a conversation on the issues relevant to your organisation, rather than a structured questionnaire.
ADD IF NECESSARY: The interviews would last no longer than 45 minutes and those taking part would be offered a £50 cheque or a donation to the charity of their choice.

SINGLE CODE
Yes
No

ASK ALL
**Q49.REPORT**
Would you like us to email you a copy of last year's report and a government help card with links to the latest official cyber security guidance for organisations like yours?

SINGLE CODE
Yes
No

ASK IF WANT RECONTACT OR REPORT (RECON CODE 1 OR REPORT CODE 1)
**Q50.EMAIL**
IF WANT REPORT (REPORT CODE 1): Can I please take an email address for this?
IF DON'T WANT REPORT (REPORT CODE 2): Can I please take an email address to invite you to the follow-up interview only?

WRITE IN EMAIL IN VALIDATED FORMAT
DO NOT READ OUT: Refused

SEND FOLLOW-UP EMAIL IF WANT REPORT AND GIVE EMAIL (REPORT CODE 1 AND EMAIL NOT BLANK)

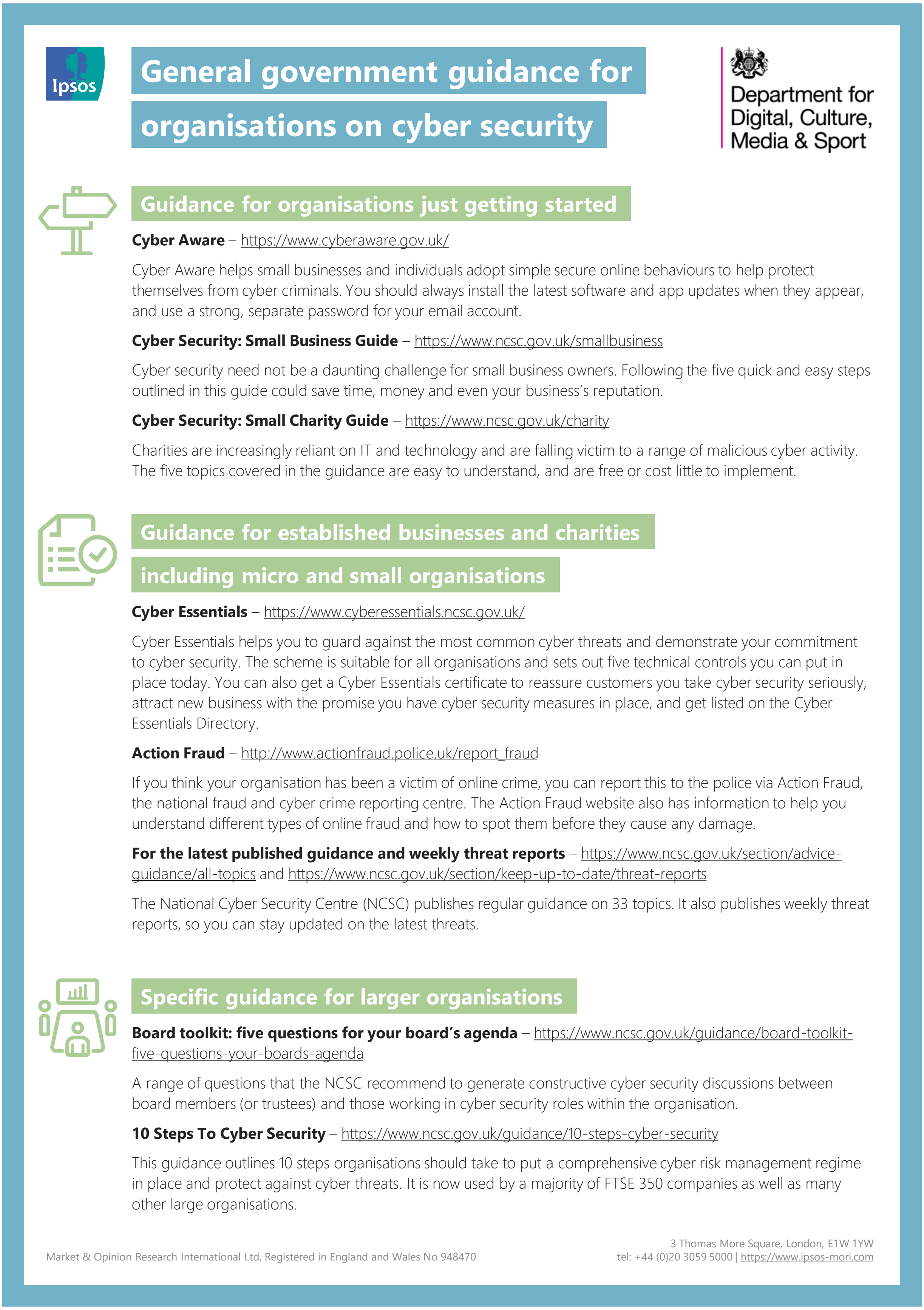
## GDPR privacy policy

READ OUT TO ALL
Thank you for taking the time to participate. You can access the privacy policy on our website at: https://ipsos.uk/12025p. This explains the purposes for processing your personal data, as well as your rights under data protection regulations to:

- access your personal data
- withdraw consent
- object to processing of your personal data
- and other required information.

CLOSE SURVEY

# Appendix B: Government help cards offered to survey respondents



## General government guidance for organisations on cyber security

Department for Digital, Culture, Media & Sport

### Guidance for organisations just getting started

**Cyber Aware** – https://www.cyberaware.gov.uk/

Cyber Aware helps small businesses and individuals adopt simple secure online behaviours to help protect themselves from cyber criminals. You should always install the latest software and app updates when they appear, and use a strong, separate password for your email account.

**Cyber Security: Small Business Guide** – https://www.ncsc.gov.uk/smallbusiness

Cyber security need not be a daunting challenge for small business owners. Following the five quick and easy steps outlined in this guide could save time, money and even your business's reputation.

**Cyber Security: Small Charity Guide** – https://www.ncsc.gov.uk/charity

Charities are increasingly reliant on IT and technology and are falling victim to a range of malicious cyber activity. The five topics covered in the guidance are easy to understand, and are free or cost little to implement.

### Guidance for established businesses and charities including micro and small organisations

**Cyber Essentials** – https://www.cyberessentials.ncsc.gov.uk/

Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security. The scheme is suitable for all organisations and sets out five technical controls you can put in place today. You can also get a Cyber Essentials certificate to reassure customers you take cyber security seriously, attract new business with the promise you have cyber security measures in place, and get listed on the Cyber Essentials Directory.

**Action Fraud** – http://www.actionfraud.police.uk/report_fraud

If you think your organisation has been a victim of online crime, you can report this to the police via Action Fraud, the national fraud and cyber crime reporting centre. The Action Fraud website also has information to help you understand different types of online fraud and how to spot them before they cause any damage.

**For the latest published guidance and weekly threat reports** – https://www.ncsc.gov.uk/section/advice-guidance/all-topics and https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports

The National Cyber Security Centre (NCSC) publishes regular guidance on 33 topics. It also publishes weekly threat reports, so you can stay updated on the latest threats.

### Specific guidance for larger organisations

**Board toolkit: five questions for your board's agenda** – https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda

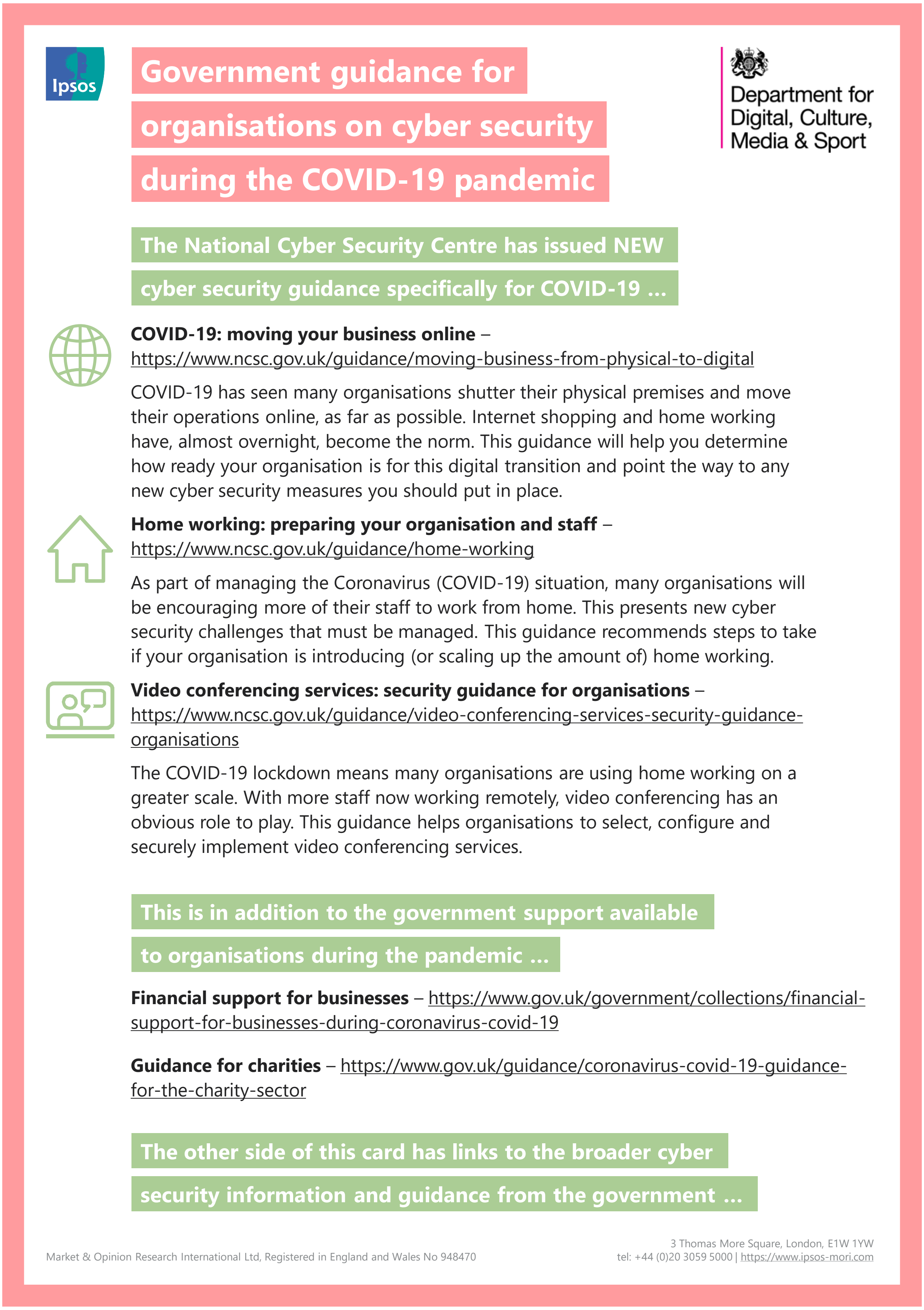
A range of questions that the NCSC recommend to generate constructive cyber security discussions between board members (or trustees) and those working in cyber security roles within the organisation.

**10 Steps To Cyber Security** – https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

This guidance outlines 10 steps organisations should take to put a comprehensive cyber risk management regime in place and protect against cyber threats. It is now used by a majority of FTSE 350 companies as well as many other large organisations.

Market & Opinion Research International Ltd, Registered in England and Wales No 948470

3 Thomas More Square, London, E1W 1YW
tel: +44 (0)20 3059 5000 | https://www.ipsos-mori.com



Ipsos

# Government guidance for organisations on cyber security during the COVID-19 pandemic

Department for Digital, Culture, Media & Sport

## The National Cyber Security Centre has issued NEW cyber security guidance specifically for COVID-19 …

**COVID-19: moving your business online** – https://www.ncsc.gov.uk/guidance/moving-business-from-physical-to-digital

COVID-19 has seen many organisations shutter their physical premises and move their operations online, as far as possible. Internet shopping and home working have, almost overnight, become the norm. This guidance will help you determine how ready your organisation is for this digital transition and point the way to any new cyber security measures you should put in place.

**Home working: preparing your organisation and staff** – https://www.ncsc.gov.uk/guidance/home-working

As part of managing the Coronavirus (COVID-19) situation, many organisations will be encouraging more of their staff to work from home. This presents new cyber security challenges that must be managed. This guidance recommends steps to take if your organisation is introducing (or scaling up the amount of) home working.

**Video conferencing services: security guidance for organisations** – https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

The COVID-19 lockdown means many organisations are using home working on a greater scale. With more staff now working remotely, video conferencing has an obvious role to play. This guidance helps organisations to select, configure and securely implement video conferencing services.

## This is in addition to the government support available to organisations during the pandemic …

**Financial support for businesses** – https://www.gov.uk/government/collections/financial-support-for-businesses-during-coronavirus-covid-19

**Guidance for charities** – https://www.gov.uk/guidance/coronavirus-covid-19-guidance-for-the-charity-sector

## The other side of this card has links to the broader cyber security information and guidance from the government …

Market & Opinion Research International Ltd, Registered in England and Wales No 948470

3 Thomas More Square, London, E1W 1YW
tel: +44 (0)20 3059 5000 | https://www.ipsos-mori.com

# Appendix C: Topic guide for cyber sector and other organisation qualitative interviews

| 1: Introduction | Timings |
|---|---|
| ▪ **Thank** participant for taking part.<br>▪ **Introduce self, Ipsos MORI:** independent research organisation; adhere to the MRS Code of Conduct which ensures our research is carried out in an ethical and professional manner, based on voluntary informed consent and that individuals' rights, wellbeing and confidentiality is respected at all times.<br>▪ **The interview:** informal conversation on their views, no right or wrong answers.<br>▪ **The research:** DCMS wants to understand in more depth current and future cyber skills gaps, and their impact on recruitment to help inform future government policy.<br>▪ **Confidentiality:** All responses are confidential and anonymous. DCMS won't know who has taken part and will get an anonymised report pulling out the key findings across all interviews. Participation is voluntary and you can change your mind at any time. Can I confirm you are happy to take part on this basis?<br>▪ **Explain GDPR conditions:** Ipsos MORI requires a legal basis to process your personal data. Ipsos MORI's legal basis for processing your data is your consent to take part in this research.<br>▪ **Explain voluntary participation:** If you wish to withdraw your consent to take part at any time, or stop the discussion for any reason, then please let us know.<br>▪ **Incentive:** £50<br>▪ **Recording:** get permission to digitally record.<br>▪ **Length:** Approx. 55-60 mins<br>▪ Any questions?<br><br>**<u>GDPR added consent (once the recorder is on)</u>**<br><br>Ipsos MORI's legal basis for processing your data is your consent to take part in this research. Your participation in this research is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview. Can I check that you are happy to proceed? | 2 minutes |
| **2: Context** | **Timings** |
| *This section aims to warm up the participant and gain context about the organisation and their role within it.*<br>**Can you tell me about your organisation?**<br>▪ What does the organisation focus on?<br>**And what is your role within the organisation?**<br>▪ PROBE around their role in recruitment and training.<br>**Background:**<br>▪ Can I ask about your career history before taking on this role?<br>▪ PROBE around whether they have a cyber security background. | 2 minutes |
| **3: Perception of skills gaps** | **Timings** |
| **<u>Current skills gaps and implications</u>** | 10-12 minutes |

| | |
|---|---|
| **Right now, what are the main challenges and gaps when it comes to cyber skills in your organisation?** PROBE ON:<br>▪ Technical skills/knowledge<br>▪ Implementation/ability to implement technical knowledge<br>▪ Non-technical skills (e.g. communication, management, people skills)<br>▪ Seniority – which positions/roles face the greatest challenges<br>**What's the impact of these skills gaps on your organisation?** What problems/issues does it create:<br>▪ For your role/in your team (PROBE on impact of being over-stretched, risk of over-promoting people etc.)<br>▪ For the wider organisation/directors<br>**What approaches has your organisation taken to deal with these skills gaps and challenges?**<br>▪ What has been most successful?<br>▪ What lessons have you learnt? What advice would you give to other organisations in your situation?<br>**How have you coped in situations where resourcing/budgets are tight or with surges in demand? How have you supported your teams through this?** PROBE around:<br>▪ Short-term solutions vs. long-term solutions<br>▪ Use of freelancers/stopgap hiring<br>▪ Staff filling multiple roles/performing multiple functions<br>▪ Welfare/support for people in your team (i.e. emotional/mental health impact)<br>▪ Internal recruitment/training or moving resources from other departments – which skills/roles transfer more/less easily? How elastic is this?<br>▪ Broadening/diversifying recruitment/training (WILL BE DISCUSSED AGAIN IN DETAIL LATER IN INTERVIEW)<br><br>**COVID-19 and remote working**<br><br>**How has the COVID-19 pandemic affected your cyber skills needs and challenges?** PROBE ON:<br>▪ Changes in demand<br>▪ Changing work patterns/environment (e.g. impact of remote working)<br>▪ Any positive impacts?<br>**What impact has remote working specifically had on cyber skills gaps?**<br>▪ Are people in cyber roles able to work remotely? PROBE on full-time/part-time remote working.<br>▪ What advantages/challenges does this bring? How have you addressed these? What has worked well/what lessons have you learnt?<br>▪ Has remote working changed who/where you can hire in cyber roles (e.g. locations of employees)? Are you already recruiting outside your geographic locations? Will it change this in the future? | |
| **4. Training** | **Timings** |
| **Training for people in cyber roles**<br><br>**How would you describe your overall approach to training and upskilling the people in cyber roles in your organisation?**<br>▪ What has worked well/what are the main lessons have you learnt?<br>▪ Have you changed any part of this training under COVID-19?<br>**What role do cyber security qualifications or certified training play?**<br>▪ How useful are these to your organisation/cyber team? Any qualifications that are particularly relevant?<br>▪ How could the current set of qualifications/certifications be improved? | 15 minutes |

### FOR LARGE ORGANISATIONS (NOT CYBER SECTOR): Cyber security training/awareness raising for wider staff

**And how would you describe your overall approach to cyber security training and raising awareness among your wider staff? Among senior management?**

- What has worked well/what are the main lessons have you learnt?
- Have you changed any part of this training under COVID-19? E.g. training around remote working? How successful has this been? Is there more left to do?

### Developing/sourcing training

**How does your organisation develop cyber security training materials for all these groups (i.e. those in cyber roles, wider staff and senior staff)?** PROBE around:

- In-house developed training vs. external training products – what is behind this choice?
- How easy is it to find the right external training? Where do you look? What does good external training look like?
- How do you quality-assure the training? How do you keep it up to date with the latest cyber security developments/knowledge?

**Have you heard of any cyber security skills or roles frameworks? Have you used any for assessing training needs or before?** PROBE on use/relevance of:

- CYBOK (Cyber Security Body of Knowledge)
- CIISec (Chartered Institute for Information Security) or IISP skills and roles frameworks
- US frameworks: NICE (National Initiative for Cybersecurity Education) and NIST cybersecurity framework
- How are these used exactly?

### Delivering training

**How does your organisation deliver cyber security training for all these groups (i.e. those in cyber roles, wider staff and senior staff)?** PROBE around:

- On-the-job vs. off-the-job training
- Grad/new joiner training vs. ongoing/continuing professional development
- Classroom vs. remote/online
- How has this changed/will this change under COVID-19? What impact will this have? What measures have you put in place?

### Training barriers/challenges

**What are the gaps in your cyber security training? What improvements would you like to see? What changes are you planning or considering?**

**What are your main challenges when it comes to cyber security training? What stops you from filling these gaps/making improvements?** PROBE on:

- Attitudes of senior management/wider staff
- Skills/time to be able to train others
- Sourcing the right training/complexity of training market
- Do you have a specific cyber security training budget/remit? What difference does this make? How does spending/time on training get approval?

**How do you evaluate the training? How do you know if it's meeting your needs?**

- Any benchmarking, e.g. of staff knowledge/awareness? Has this been going up/down?

### Role of government

**What role should the government play in supporting cyber security training and upskilling in organisations like yours? What support can it offer?**

**Have you heard of any government-sponsored schemes for cyber security skills and training? PROBE on awareness/views of:**

- Cyber First/Cyber Discovery
- The Skills Toolkit

| **5: Cyber recruitment** | **Timings** |
|---|---|
| **<u>Recruitment approaches</u>**<br>**How would you describe your overall approach to recruiting people into cyber roles in your organisation?**<br>▪ Where/how do you post jobs?<br>▪ Do you try to recruit people who are job-ready, or people who you can train up? How realistic is it to find job-ready people for all the cyber roles you need?<br>**How flexible/tailored is your recruitment approach?**<br>▪ How has this changed over time? How willing is your organisation to test new approaches? What has been more/less successful?<br>▪ FOR LARGE FIRMS (NOT CYBER SECTOR): Do you have to stick to the same approaches for cyber recruitment that are used for other roles in the organisation? E.g. same recruitment agents, job postings etc. How tailored is the recruitment approach to your cyber team specifically?<br>**How do you work with recruitment agents to fill cyber roles? How well do they understand/meet your needs?** PROBE ON:<br>▪ Technical knowledge, understanding of your organisation, understanding local market, calibre of candidates received<br>▪ How do you communicate/meet with them? How do they find out what you need/want?<br>▪ How did you choose this recruitment agency? What do they do well/less well?<br>**How do you work with HR teams/colleagues to fill cyber roles? How well do they understand your needs?** PROBE AS ABOVE.<br>**Who writes the job descriptions/ads?**<br>▪ Do you get any support with this from recruitment agents/HR? Do you get any feedback? Have you made any changes/improvements?<br>▪ How easy are these to write?<br>▪ What do you use/look at to support you (e.g. matching job ads from other companies, using roles/skills frameworks)?<br>**How do you try to attract candidates? What are your USPs? Which aspects are harder to compete on?**<br>▪ PROBE on salaries, location, career development/training offer, workplace culture.<br>**What internal recruitment do you do to fill cyber roles?**<br>▪ What roles is this best suited to? Any particular roles where skills transfer easily? Anywhere this does not work well?<br>▪ What role do HR colleagues play in this?<br>**What's your approach to apprenticeships in cyber roles?**<br>▪ What apprenticeship standards/frameworks have you used?<br>▪ How successful has this been? What challenges have you faced?<br>▪ IF NOT USING APPRENTICESHIPS: Have you looked into this? What's stopping you from using apprenticeships? What was behind that decision?<br>**<u>Minimum recruitment criteria</u>**<br>**Do you have minimum recruitment criteria for cyber roles?** PROBE on:<br>▪ Education requirements, qualifications, years of experience<br>▪ How flexible are you with these criteria? Have you changed them in the past? Do any of these minimum requirements make it harder to find candidates?<br>**<u>General recruitment challenges</u>**<br>**What have the main challenges been when recruiting people for cyber roles?** | 20 minutes |

| | |
|---|---|
| ▪ What kinds of recruitment are most challenging? E.g. different job roles, specialisms, seniority levels.<br>**What has made cyber roles hard to fill in the past? Tell me about any recent posts that have been hard to fill.**<br>▪ USE THIS SECTION TO BUILD A BRIEF CASE STUDY OF ANY RECENT HARD-TO-FILL POSTS. PROBE on nature of role, where/how long advertised, methods of recruitment used, whether eventually filled, specific challenges/issues.<br>▪ How did you get around this? Did you change your approach in response? What worked/what lessons have you learnt?<br>**How does your location impact your organisation's ability to recruit for cyber roles?**<br>▪ What kinds of candidates do you tend to get more/less of in this geographic area?<br>**How does your size impact your ability to recruit?**<br>▪ PROBE on perceived impact of larger firms, especially large cyber consultancies, on jobs market.<br><br>**<u>COVID-19 and recruitment</u>**<br><br>**How has COVID-19 impacted your recruitment?** PROBE on impact on:<br>▪ Recruitment budgets, local labour markets/applicants, salary demands<br>▪ Have you changed/will you change your recruitment approaches as a result? What will you have to do more/less of?<br>**Have you recruited/will you recruit staff who can work remotely?**<br>▪ Will this change the locations you recruit from?<br>▪ What implications does this have for your recruitment approach?<br><br>**<u>Role of government</u>**<br><br>**What role should the government have in supporting recruitment for cyber roles in organisations like yours?**<br>▪ What steps could they take? What support could they offer? | |
| **6: Diversity in cyber teams** | **Timings** |
| **What do you think I mean when I talk about diversity in the cyber sector/in cyber teams?**<br>▪ What kinds of characteristics do you think this refers to? What ones are most important?<br>▪ How big an issue is this for the cyber sector, in your opinion? What kinds of diversity do you think are lacking?<br>▪ Where do you hear about this? What has informed your opinions on this topic?<br>**How important a consideration is diversity in your cyber teams?**<br><br>▪ Probe on: Socioeconomic diversity; Ethnic diversity; Gender diversity; people with disabilities; People with neurodiverse conditions.<br>▪ How does it factor into recruitment approaches/promotions? Is this a formal consideration/following a policy, or just considered informally?<br>▪ FOR LARGE FIRMS (NOT CYBER SECTOR): Does your organisation look at this issue specifically for cyber teams, or just at an organisation-wide level? Do you take specific action for cyber teams?<br>**How diverse are your cyber teams? What about senior cyber roles vs. junior cyber roles?**<br>▪ How do you measure this? What are your criteria for a diverse cyber team? Do you have formal measures? Do you consider it by grade/seniority, by salary band, or just at an overall level?<br>**What impact does it make having a more diverse cyber team?** FIRST ASK WITHOUT PROMPTING AND THEN PROBE on:<br>▪ What would you say is the top impact/main reason to aim for a more diverse cyber team? | 15 minutes |

| | |
|---|---|
| ▪ Impact on skills gaps/shortages – before this interview, had you considered a more diverse workforce as a way of filling your skills gaps/shortages?<br>**How diverse are the people applying to you for cyber jobs?**<br>▪ How responsible do you think organisations like yours are when it comes to the diversity of people applying? What control do you have over this? Do you think you do enough?<br>**What actions have you taken to improve diversity in your cyber teams?**<br>▪ What steps have you taken in terms of recruitment approaches/increasing the diversity of job applicants?<br>▪ What has guided this – where did you find out about the changes you could make?<br>▪ Do you know what kinds of actions you should be taking? Do you know if you're following best practice?<br>**Are you aware of any government initiatives to improve diversity in the cyber workforce?** PROBE on awareness/opinions of:<br>▪ The Tech Talent Charter, Cyber Discovery, Cyber First, Cyber First Girls Competition | |
| **7: Future skills needs** | **Timings** |
| **What skills do you think you will need more of in 3 years' time? In 5 years' time? Why are these becoming more important?**<br>▪ Do you feel gaps in cyber skills are likely to get better or worse? Why?<br>▪ What impact would it have if you didn't get these skills in the future?<br>▪ What steps is your organisation taking in relation to this?<br>**What role does government have in addressing these upcoming skills needs?**<br>▪ How can they best support cyber teams like yours with upcoming skills needs? | 5 minutes |
| **8: Wrap-up** | **Timings** |
| **Overall, what do you think is the one thing we should tell the government from this interview, to ensure the cyber skills labour market meets the needs of your organisation?**<br>**Finally, if you have one piece of wisdom that you wish you could share with other organisations like yours when it comes to cyber skills, what would it be?**<br>THANK PARTICIPANT AND CLOSE INTERVIEW. REMIND THEM OF CONFIDENTIALITY. | 2 minutes |

# Appendix C: Topic guide for recruitment agent qualitative interviews

| 1: Introduction | Timings |
|---|---|
| ▪ **Thank** participant for taking part.<br>▪ **Introduce self, Ipsos MORI:** independent research organisation; adhere to the MRS Code of Conduct which ensures our research is carried out in an ethical and professional manner, based on voluntary informed consent and that individuals' rights, wellbeing and confidentiality is respected at all times.<br>▪ **The interview:** informal conversation on their views, no right or wrong answers.<br>▪ **The research:** DCMS wants to understand in more depth current and future cyber skills gaps, and their impact on recruitment to help inform future government policy.<br>▪ **Confidentiality:** All responses are confidential and anonymous. DCMS won't know who has taken part and will get an anonymised report pulling out the key findings across all interviews. Participation is voluntary and you can change your mind at any time. Can I confirm you are happy to take part on this basis?<br>▪ **Explain GDPR conditions:** Ipsos MORI requires a legal basis to process your personal data. Ipsos MORI's legal basis for processing your data is your consent to take part in this research.<br>▪ **Explain voluntary participation:** If you wish to withdraw your consent to take part at any time, or stop the discussion for any reason, then please let us know.<br>▪ **Recording:** get permission to digitally record.<br>▪ **Length:** Approx. 60-75 mins (x1) OR Approx. 35-45 mins (x2)<br>▪ **Any questions?**<br><br>**<u>GDPR added consent (once the recorder is on)</u>**<br><br>Ipsos MORI's legal basis for processing your data is your consent to take part in this research. Your participation in this research is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview. Can I check that you are happy to proceed? | 5 minutes |
| **2: Context** | **Timings** |
| *This section aims to warm up the participant and gain context about the organisation and their role within it.*<br>**To start with, tell me a bit about your organisation and your role within it.**<br>▪ How long have you been with the organisation?<br>▪ How long have you worked or been involved in cyber security recruitment?<br>▪ What other sectors, if any, do you deal with?<br>▪ What regions within the UK do you recruit for?<br><br>**And what is your role within the organisation?**<br>▪ What are your day-to-day tasks?<br>▪ If you have a team, please describe it to us.<br>▪ How many years of experience does your team have in recruitment in general?<br>▪ How many years of experience does your team have in cyber security recruitment?<br>▪ How specialised are you with Cyber Skilled recruitment?<br>- Do you focus on a particular position/skill?<br>- Was this a conscious decision or did it arise organically? | 5-10 mins |

| | |
|---|---|
| **Background:**<br>- Do you have a technical or academic background in Cyber Security/IT?<br>- **If no**, can you tell me how you learnt about the sector?<br>- Did they learn about the sector on the job?<br>- Take formal training?<br>- Support from colleague around terminology?<br>- **If yes**, how beneficially was this background?<br>- Were the skills transferable? | |
| **3: Current Cyber Security candidate pool** | **Timings** |
| *This section explores the current supply of cyber security talent in the UK, how they find their way into roles, and what the candidate pool looks like*<br>**Approximately, how many active (i.e. actively looking to get a/move jobs) and passive (i.e. not actively looking to get a/move jobs) cyber candidates do you have in your books?**<br>▪ Have these numbers changed recently? E.g., due to COVID-19.<br>▪ What is the typical experience and education these cyber skills candidates have?<br>▪ Where are they based geographically?<br>▪ If you got given a role by your client to work on, approximately how many candidates from your books would you be able to call immediately? How does this differ by role?<br>**Describe the most and least effective methods you/your team use to source good quality cyber candidates? (e.g., Linkedin, Indeed)**<br>▪ What other methods are available to you?<br>*If more than two mentioned, probe on what order they would put them in (from most effective, to least effective).*<br>**What characteristics (or features?) in a cyber role and/or company do you find are most compelling for candidates?**<br>▪ How does this differ between candidates with a cyber background and a non-cyber background?<br>**In a typical working week, how many cyber candidates do you/does your team proactively try to recruit for your books (e.g., headhunt)?**<br>▪ Are they from other career paths (non-cyber)? If so, where?<br>▪ Are they from cyber career paths? If so, what field (e.g. pen testing)?<br>**What are the typical reasons candidates give you when they're looking to leave their current role?**<br>▪ What proportion of these candidates are in cyber?<br>▪ What proportion of these candidates are looking to get in to cyber?<br>▪ Probe on industry and size of companies<br>**What are the typical reasons candidates give you when they're interested in a new cyber role?**<br>▪ What proportion of these candidates are in cyber?<br>▪ What proportion of these candidates are looking to get in to cyber?<br>▪ Probe on industry and size of companies | 25-30 mins |

| | |
|---|---|
| **If you recruit cyber entry-level roles, please summarise the typical profile of candidates that show interest in applying in terms of educational background, specialisms and region.**<br>▪ If at all, how do they differ to the typical profile of candidates you shortlist to send your client?<br>▪ What are the reasons further/higher education leavers give for looking for a job in cyber security? What kind of courses are they coming from?<br>▪ If at all, how does the pool of candidates who are further/higher education leavers vary geographically?<br>▪ What kind of apprenticeships or degree level apprenticeship will they have done/ are offered to them?<br>**How has the pool changed over the past five years? How is it likely to change in the next five years? Why?**<br>▪ What about the educational background in the pool? How is this changing? Is it more academic focused (e.g. candidates with Masters), or focused on more professional qualifications?<br>▪ How are specialisms changing? Why is this? How will it change further?<br>▪ How has the regional landscape changed? To what extent will more home working affect this?<br>**Which sectors/industries are competing with cyber security and related fields for employees?**<br>▪ What are the other sectors that employees/potential employees within cyber security may choose to move to? Why? What does this mean for the employer?<br>▪ Who is the most/least likely to choose cyber security over these competing sectors? Why? What impact does this have on the pool?<br>**How have recent disruptive events affected the candidate pool?**<br>▪ How might it/they in the future?<br>▪ **What about COVID-19?** How has the pandemic affected the pool and how do you think it might impact the pool in the future?<br>▪ **And what about Britain's exit from the EU specifically?** How has this affected the pool? How might it impact the pool in the future?<br>▪ **If there has been a change in the size of the candidate pool (e.g., increase of candidates in the job market), what is the ratio of suitable vs. unsuitable candidates (displaced candidates) for roles at the moment?** | |
| **4: Diversity of the cyber candidate pool & in cyber recruitment** | **Timings** |
| *Next, we would like to understand the diversity of the current candidate pool and caveat that by diversity we mean: being from a minority ethnic background; gender balanced; having a physical disability, that is, any long-standing illness, condition or impairment, which causes difficulty with day-to-day activities; and a neurodiverse condition or learning disorder, such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD).*<br>**How would you describe the diversity of the candidate pool currently available?**<br>▪ How often are they from the same background (e.g. same university, type of degree)? If so, why do you think that is?<br>▪ What proportion of the candidates you speak/work with are from:<br>- BAME backgrounds? Which ethnic groups are more/less represented?<br>- What about female vs. male?<br>- And neurodiversity candidates?<br>- And candidates with physical disability? | 10-15 mins |

- **In your opinion, is there a trend with this or is it stagnant?** Why do you think this is?

**If at all, do you do anything to proactively encourage candidates with these characteristics to enter/continue in cyber?** E.g. altering communication styles, application processes, where you recruit from etc.

**What do you see as your role in this area?** Do you feel that recruiters have any responsibilities in this area? If so, can you tell me about them? If any, can you provide examples of best practice and do agents have a role in proliferating these?

**For a typical role you work on, of the shortlist you send to your client how many of these are from a BAME background, female, have a neurological or physical disability?**

- How does this change if the role you are shortlisting for is a senior position, e.g., a Cyber Security Officer or Director?

**Are there any diversity quotas clients ask for on the shortlisted candidates? Is it HR or the cyber hiring manager who ask for this?**

- Are there any diversity quotas clients are trying to meet internally?

**What reasons, if any, might candidates from diverse groups be unsuccessful?**

- What barriers, if any, do you see to overcoming these issues
- What do you think can be done to overcome this? Please provide any examples.

| **5: Recruitment Criteria** | **Timings** |
|---|---|
| | 10 -15 mins |

**What do your clients typically look for in candidates? And are there any role specific requirements?**

- How do you weight the different factors?
- What traits are harder to come by?
- How does this vary according to type of job role?
- How does this vary according to location?

*PROBE AS MUCH AS POSSIBLE ON:*
*EXPERIENCE VS. SENIORITY VS. QUALIFICATIONS*
*TECHNICAL VS. COMPLEMENTARY SKILLS VS. OTHER QUALITIES*
*SPECIALIST VS. GENERALIST SKILLS*

- How realistic are these employer demands to meet from the current cyber candidate pool?

**How easy is it to define which skills your clients look for in their roles?**

- And how easy is it to assess whether candidates have these skills?
- [IF NOT TECH SKILLS NOT YET MENTIONED] How easy is it to assess candidates' technical expertise at screening?

**What kind of formal qualifications do your clients look for and what do they accept?**

- Of the candidates you have placed recently, what qualifications did they have versus what was the client asking for initially?
- How do you and your team keep up to date with the array of cyber qualifications available?
- What is the demand for higher education cyber courses?

*Probe on minimum educational requirements, cyber certifications, and what stands out in the job market*

**Typically, how many years of experience do your clients look for and what do they accept?**

| | |
|---|---|
| ▪ Of the candidates you have placed recently, how many years of cyber and/or non-cyber experience did they have, versus what was the client asking for initially?<br>▪ How do you and your team keep up to date with the array of cyber career pathways?<br><br>**What makes candidates stand out when discussing cyber/non-cyber candidates with cyber hiring managers?**<br>▪ What's the difference between successful and unsuccessful candidates?<br>▪ Do hiring managers lean more towards technical skills, or more non-technical [complementary] skills, such as communication, management and teamwork? | |
| **6: Current cyber recruitment** | **Timings** |
| **What would you say are the key issues/challenges in recruiting people for Cyber Security roles?**<br>▪ Do these vary:<br>▪ Depending on the level of experience required? (e.g., entry-level, associate, senior manager, etc)<br>▪ Do these vary geographically?<br>▪ Probe on type of client<br><br>**Are there cyber roles:**<br>***a)*** **In which candidates tend to stay less time in?**<br>***b)*** **You tend to recruit more of?**<br>**Are there any geographical differences in (a) and (b)?**<br>*E.g., London, Birmingham, Manchester, Edinburgh and Bristol people move between roles quicker?*<br>▪ Probe on type of client<br><br>**Have there been any particular roles/grades that you have found more challenging to fill?**<br>▪ How have you dealt with these?<br>▪ Have you changed your approach with your clients?<br>▪ What has worked well?<br>▪ What remains a challenge?<br><br>**Roughly, what is your ratio of CVs. sent: Interview; Interview: Job offer, and job offer: Job offer accepted? How does this differ by seniority level?**<br>▪ For each stage, what are the most common barriers you find in a cyber recruitment process?<br>▪ How long can a recruitment process take to complete?<br><br>**How do the salaries offered for cyber specialists typically differ to those offered to other kinds of technical roles (e.g. technical IT roles)?**<br>▪ What kinds of challenges or pressures does this create?<br>▪ How do you deal with this and manage your clients?<br><br>**How often do the roles you recruit for go internal?**<br>▪ What are the reasons for this?<br><br>**In your experience, have people come from other sectors to work in the cyber sector?**<br>▪ What are the advantages/drawbacks that these groups tend to face?<br><br>**How do skills from different sectors cross over into the Cyber sector?**<br>*Probe around: Technical/Hard Skills, complementary skills, experience (later career applicants)* | 15-20 mins |

| | |
|---|---|
| **[IF NOT ASKED ABOUT BREXIT IN SECTION 4] Has Brexit provided any challenges and opportunities in terms of recruiting Cyber Security roles?**<br>▪ What impact do you think it will have in the future?<br><br>**[IF NOT ASKED ABOUT COVID-19 IN SECTION 4] Has COVID-19 provided challenges and opportunities in terms of recruiting Cyber Security roles?**<br>▪ What impact do you think it will have in the future? | |
| **7: Recruitment approaches** | **Timings** |
| **In relation to recruiting in the cyber sector, do you try to keep up to speed with developments in cyber skills and the kinds of skills/knowledge employers want?**<br>▪ If so, how do you do this?<br>▪ If not, what are the barriers to keeping up to date? Has this ever hindered recruitment with a position?<br><br>**Have you ever used any frameworks when recruiting for a cyber skills position?** If so, which one(s)? Probe around awareness of CyBOK?<br><br>**Do you use any other resources in your recruitment approach?** Probe around NSCS, NIST, others<br><br>**Moving onto relationships with hiring manager, typically how do you find these relationships? Describe what a warm and a cold relationship is like.**<br>▪ How easy is it to build strong relationships with cyber clients?<br>▪ Approx., how much time does your team need to spend on business development per week?<br>▪ Can you talk me through a positive example of how a positive relationship helped fill a cyber position?<br>▪ Can you talk me through a negative example now?<br><br>**Typically, how are your relationships with HR? Describe what a positive and a negative relationship is like.**<br>▪ What is HR's relationship with the hiring cyber teams like?<br><br>**How do you find the quality of CV and interview feedback?**<br><br>**Has the way your cyber clients' recruit changed over the last three years?**<br>▪ If so, how?<br>▪ To what extent are your clients willing to use new approaches, even if these are untested?<br>*Prompt on willingness to accept unqualified or limited experience.*<br><br>**What sort of changes to the recruitment approach would you like to see in the future/you think are necessary?** | 10 -15 mins |
| **8: Wrap-up** | **Timings** |
| **What role does the Government have in making it easier to recruit new staff for Cyber Security roles?**<br>▪ What steps could they take?<br>▪ What support could they offer?<br><br>**If further guidance of cyber career pathways, qualifications and training could be provided to the recruitment sector, what should that look like?**<br>*Probe on all three.* | 3-4 mins |

| | |
|---|---|
| **What support government and industry could offer to ensure the recruitment pool can serve the needs of employers?**<br>**How can the supply of labour be improved and/or increased to satisfy demand?**<br>*Thank participant and close interview. Remind them of confidentiality.* | |

# Appendix E: Inclusion/exclusion criteria for job vacancies analysis

We developed the search string below to identify job postings for technical cyber job role and cyber-enabled roles on the Burning Glass Technologies database, after following the process laid out in Chapter 6. The first part of the string, presented in **black text**, specifies the *included* search terms across the job postings search. The second part of the string, presented in **red text**, specifies the *excluded* terms across job postings search. Please note, this search consciously includes partially spelled words and, in some cases, spelling errors. This reflects common spelling errors across these job postings.

Search Strategy (All*)

UK-wide AND ( Title with : Security Engineer OR Title with : Security Manager OR Title with : Security Consultant OR Title with : Security Architect OR Title with : Security Analyst OR Title with : Network Engineer OR Title with : Information Security Manager OR Title with : Information Security Analyst OR Title with : Cyber OR Title with : Trainee Cyber Security OR Title with : Network Architect OR Title with : Information Security Officer OR Title with : Information Technology Auditor OR Title with : Security Specialist OR Title with : Cyber Security Engineer OR Title with : Network Security Engineer OR Title with : Information Security Consultant OR Title with : Information Technology Security Analyst OR Title with : Cyber Security Trainee OR Title with : Cyber Security Specialist OR Title with : Penetration Tester OR Title with : Information Security Specialist OR Title with : Data Protection Officer OR Title with : It Security Trainee OR Title with : Information Security Engineer OR Title with : Information Governance Officer OR Title with : Risk Analyst OR Title with : Information Security Architect OR Title with : Soc Analyst OR Title with : Head Of Information Security OR Title with : Senior Infrastructure Engineer OR Title with : Senior Penetration Tester OR Title with : Trainee Cyber Security Support Technician OR Title with : Cyber Resilience Manager OR Title with : Senior Soc Analyst OR Title with : Head Of It Security OR Title with : Cisco Engineer OR Title with : Network Specialist OR Title with : Network Analyst OR Title with : Network Administrator OR Title with : Cyber Security Apprentice OR Title with : Cyber Security Lead OR Title with : Chief Information Officer OR Title with : Data Protection Lead OR Title with : Information Security Auditor OR Title with : Junior Penetration Tester OR Title with : Vulnerability OR Title with : threat OR Title with : Authorizing Official/Designating Representative OR Title with : Security Control Assessor OR Title with : Secure Software Assessor OR Title with : System Testing and Evaluation Specialist OR Title with : Information Systems Security Developer OR Title with : Network Operations Specialist OR Title with : System Administrator OR Title with : Systems Security Analyst OR Title with : Cyber Legal Advisor OR Title with : Privacy Officer OR Title with : Cyber Instructional Curriculum Developer OR Title with : Cyber Instructor OR Title with : Communications Security (COMSEC) Manager OR Title with : Cyber Workforce Developer and Manager OR Title with : Cyber Policy and Strategy Planner OR Title with : Executive Cyber Leadership OR Title with : Cyber Defense Analyst OR Title with : Vulnerability Assessment Analyst OR Title with : Exploitation Analyst OR Title with : All-Source Analyst OR Title with : Mission Assessment Specialist OR Title with : Target Network Analyst OR Title with : Cyber Ops Planner OR Title with : Cyber Intel Planner OR Title with : Cyber Crime Investigator OR Title with : Forensics Analyst OR Title with : CISO OR Title with : Chief Information Security Officer OR Title with : & Perimeter OR Title with : 1st 2nd OR Title with : 1st and 2nd OR Title with : 1st Level OR Title with : 1st Line OR Title with : 1st/2nd IT Line OR Title with : 1st/2nd Line OR Title with : 2 Factor OR Title with : 27001 Assessor OR Title with : 27001 Auditor OR Title with : 2nd 3rd Line OR Title with : 2nd Line OR Title with : 2nd/3rd Line OR Title with : 3rd Infrastructure OR Title with : 3rd Level OR Title with : 3rd Party Assurance OR Title with : 3rd Party External Auditor OR Title with : 3rd Party Risk OR Title with : 3rd/4th Line OR Title with : 4th Line OR Title with : NOC Analyst OR Title with : SOC Specialist OR Title with : Pen Tester OR Title with : Computer Networking OR Title with : Hardware Security OR Title with : Security Architecture OR Title with : Product Testing Analyst OR Title with : CISCO OR Title with : Network Security OR Title with : Blockchain Solutions Architect OR Title with : Information Security Risk Lead OR Title with : Protective Monitoring Analyst OR Title with : Access Control Specialist OR Title with : Access & Identity Access OR Title with : Access & Identify Management OR Title with : Access Analyst OR Title with : Access and Identity Management OR Title with : Access and Identify Product OR Title with : Access Control Analyst OR Title with : Access Controls OR Title with : Access Database Update OR Title with : Access Management OR Title with : Active Directory OR Title with : Advanced Monitoring And Data Hunting Specialist OR Title with : Application Penetration Testing OR Title with : Application Security OR Title with : Application Services OR Title with : Application Solutions OR Title with : Application Specialist OR Title with : Application Support OR Title with : Applications Architect OR Title with : Applications Security OR Title with : Apprentice - Information Security OR Title with : Apprentice - Information Technology OR Title with : Apprentice - It OR Title with : Apprentice Ict Technician OR Title with : Apprentice IT OR Title with : Arcsight OR Title with : IT Security OR Title with : Cyber Security OR Title with : cybersecurity OR Title with : IT/Digital Security OR Title with : Arksight OR Title with : Associate Security OR Title with : Associate Software OR Title with : Associate Systems Engineer OR Title with : Associate Technical Support Engineer OR Title with : Associate Technician Support Engineer OR Title with : Forensic Technology OR Title with : Network Infrastructure OR Title with : Securing Testing OR Title with : Attack Monitoring OR Title with : Authentication OR Title with : Information Security OR Title with : Azure Security OR Title with : Backend Java OR Title with : Backend Php OR Title with : Backend Python OR Title with : National Security Academy OR Title with : Networking & Security OR Title with : Security & Networking OR Title with : Identify Governance OR Title with : Identity Management OR Title with : Blackrock Security OR Title with : Cryptographic OR Title with : Cryptography OR Title with : Identify & Access OR Title with : Identity Access OR Title with : Q Radar OR Title with : Business Continuity OR Title with : Identity & Access OR Title with : Information Risk OR Title with : Data Protection and Information Governance OR Title with : Business Resilience OR Title with : Ethical Hacker OR Title with : Incident Management OR Title with : Information Systems Auditor OR Title with : Incident Response OR Title with : Penetration Testing OR Title with : Check Point OR Title with : Check Team OR Title with : Checkpoint OR Title with : Identity Architect OR Title with : Chief Security OR Title with : Cloud Identity OR Title with : Cloud Infrastructure OR Title with : Cloud Networking OR Title with : Cloud Security OR Title with : CompTIA OR Title with : Computer Forensic OR Title with : Computer Forensics OR Title with : Computer Information Systems OR

Title with : Computer Network Defense OR Title with : Computer Network Operation OR Title with : Computer Network Operations OR Title with : Networks and Security OR Title with : Computer Security OR Title with : SIEM OR Title with : CREST OR Title with : Critical National Infrastructure OR Title with : Crypto Security OR Title with : Cryptosecurity OR Title with : CSIIP OR Title with : CSIRT OR Title with : CSOC OR Title with : Cyberark OR Title with : Cyberdefense OR Title with : Encryption OR Title with : Data Leakage OR Title with : Data Loss OR Title with : Data Management Specialist OR Title with : Data Networks OR Title with : Data Network OR Title with : Incident Lead OR Title with : Data Privacy OR Title with : Data Protection OR Title with : Data Security OR Title with : Devsec OR Title with : Devsecops OR Title with : Digital Forensic OR Title with : Digital Forensics OR Title with : Digital Governance OR Title with : Digital Privacy OR Title with : Digital Security OR Title with : Compliance and Information Security OR Title with : Information Protection & Privacy OR Title with : Payment Security OR Title with : DLP OR Title with : Edisclosure OR Title with : ediscovery OR Title with : e-discovery OR Title with : End Point OR Title with : Endpoint OR Title with : Ethical Hacking OR Title with : Ethical Security OR Title with : Firewall OR Title with : Forcepoint OR Title with : Forensic OR Title with : Forensics OR Title with : Forgerock OR Title with : Fortinet OR Title with : Gateway Security OR Title with : GDPR OR Title with : General Data Protection Regulation OR Title with : General Data Protection Regulations OR Title with : GSOC OR Title with : Managed Security Services OR Title with : Pen Testing OR Title with : Platform Security OR Title with : Security Assurance OR Title with : Security Compliance OR Title with : Security Consultancy OR Title with : Security Engineering OR Title with : Security Governance OR Title with : Security Intelligence OR Title with : Security Management OR Title with : Security Network OR Title with : Security Operations OR Title with : Security Technologies OR Title with : Security Testing OR Title with : Security, Risk OR Title with : Security, Systems OR Title with : Technical Security OR Title with : Iam OR Title with : IBM Security OR Title with : ICT Infrastructure OR Title with : ICT Network OR Title with : ICT Security OR Title with : ICT Technical OR Title with : Idam OR Title with : Identify OR Title with : Identity & Authentication OR Title with : Identity & Information OR Title with : Identity & Protection OR Title with : Identity & Risk OR Title with : Identity and Access OR Title with : Identity Authentication OR Title with : Identity Engineer OR Title with : Identity Governance OR Title with : Incident Analyst OR Title with : Information Assurance OR Title with : Information Compliance OR Title with : Information Governance OR Title with : Information Management OR Title with : Information Protection OR Title with : Information Sec OR Title with : Infrastructure Security OR Title with : ISMS OR Title with : IT - Security OR Title with : it & security OR Title with : IT Access OR Title with : IT Analyst OR Title with : IT Assurance OR Title with : IT Audit OR Title with : IT Auditor OR Title with : IT Compliance OR Title with : IT Engineer OR Title with : IT Governance OR Title with : IT Infrastructure OR Title with : IT Network OR Title with : IT Networking OR Title with : IT Networks OR Title with : IT Risk OR Title with : IT Systems OR Title with : IT Technical OR Title with : JOC OR Title with : Joint Operations OR Title with : Joint Security OR Title with : Junior Privacy OR Title with : Junior Security OR Title with : SOC OR Title with : NOC OR Title with : Juniper OR Title with : Linux OR Title with : Logrhythm OR Title with : malware OR Title with : McAfee OR Title with : Mobile Security OR Title with : Network & Security OR Title with : Network Administration OR Title with : Network and Cloud OR Title with : Network and Cryptographic OR Title with : Network and Endpoint OR Title with : Network and Firewall OR Title with : Network Consultant OR Title with : Network Engineering OR Title with : Network Lead OR Title with : Network Manager OR Title with : Palo Alto OR Title with : PCI Compliance OR Title with : PCI Consultant OR Title with : PCI DSS OR Title with : PCI QSA OR Title with : PCI:DSS OR Title with : PCI-DSS OR Title with : PCI-QSA OR Title with : Pen Test OR Title with : Penetration Test OR Title with : Penetration Testers OR Title with : Qradar OR Title with : Red Hat OR Title with : Red Team OR Title with : Blue Team OR Title with : Sailpoint OR Title with : Sap Security OR Title with : Security Incident OR Title with : Security Monitoring OR Title with : Single Sign On OR Title with : Site Reliability Engineer OR Title with : Site Reliability Engineering OR Title with : SNOC analyst OR Title with : Splunk OR Title with : Symantec OR Title with : Web Application OR Title with : Web Authentication OR Title with : Web Filtering ) AND ( Jobs in : Cybersecurity ) AND NOT ( Title with : ACA Training OR Title with : Academy Tutor OR Title with : Access Officer OR Title with : Access to Information OR Title with : Accommodation OR Title with : Account Administrator OR Title with : Account Coordinator OR Title with : Account Developer OR Title with : Account Director Wholesale OR Title with : Account Executive OR Title with : Account Handler OR Title with : Account Manager OR Title with : Accountant OR Title with : Accounting Services OR Title with : Accounts OR Title with : Acquisition Manager OR Title with : Actor OR Title with : Actuarial OR Title with : Actuary OR Title with : Ad/Sad OR Title with : Administration OR Title with : Administration Assistant OR Title with : Administration Executive OR Title with : Administrative OR Title with : Administrator OR Title with : Adminstrator OR Title with : Adobe Data OR Title with : Adobe Quality OR Title with : Adult Safeguarding OR Title with : Advertising OR Title with : AECOM OR Title with : AFC Band 3 OR Title with : Affordability OR Title with : Agent OR Title with : Aggregation Risk OR Title with : Aig Life Uk - Senior Risk Analyst OR Title with : Air Cargo OR Title with : Air Conditioning OR Title with : Aircraft OR Title with : Airport Security OR Title with : Airport/Duty Security OR Title with : Airside Security OR Title with : Alarm OR Title with : Alcentra OR Title with : Allocation Support Officer OR Title with : ALM Risk OR Title with : Alm/ OR Title with : Alpha Network Data Analyst OR Title with : AML OR Title with : AML / KYC OR Title with : AML Compliance OR Title with : Analogue Engineer OR Title with : Analyst - Business Development OR Title with : Analyst - Business Operations OR Title with : Analyst - Risk & Valuations Data Quality OR Title with : Analyst Programme OR Title with : Analyst Risk OR Title with : Analyst Screening OR Title with : Analyst Specialism OR Title with : Analyst Technology Controls OR Title with : Analyst U1 OR Title with : Analyst with Audit OR Title with : Analyst, Risk Information Services OR Title with : Analyst, Uk Network OR Title with : Analyst/Senior Analyst, Business Security Quality, Risk And Security OR Title with : Analyst/Sql/Open Source Technician/Financial E-Commerce. OR Title with : Analytical Consultant, Bens OR Title with : Analytical Risk Analyst OR Title with : Analytical Stability Scientist OR Title with : Analytical Support OR Title with : Analytics Manager OR Title with : Anatomy OR Title with : Ancillary Premises Officer OR Title with : And Risk Analyst OR Title with : ANL Risk Analyst OR Title with : Anti - Money Laundering Officer OR Title with : Anti Money Laundering OR Title with : Anti-Bribery OR Title with : Anti-Money Laundering OR Title with : Appointment OR Title with : Apprentice - Data Analyst OR Title with : Apprentice - Learning Mentor OR Title with : Apprentice Business OR Title with : Apprentice Care OR Title with : Apprentice Catering OR Title with : Apprentice CCTV OR Title with : CCTV OR Title with : Apprentice Claims OR Title with : Apprentice Collections OR Title with : Customer OR Title with : community OR Title with : Data Analyst OR Title with : Data Processor OR Title with : Designer OR Title with : Electrical OR Title with : Gas OR Title with : Joiner OR Title with : Fire OR Title with : Management Consultant OR Title with : Receptionist OR Title with : Service Centre OR Title with : Support manager OR Title with : Copywriter OR Title with : Volunteer OR Title with : Area Manager OR Title with : sales OR Title with : art OR Title with : asbestos OR Title with : Assembly OR Title with : Asset and Risk OR Title with : Asset Control OR Title with : Asset Engineer OR Title with : Asset Finance OR Title with : Asset Information Data Analyst OR Title with : Asset Liability OR Title with : Asset Management OR Title with : Asset Manager OR Title with : Asset Risk OR Title with : Asset Security Manager OR Title with : Asset Wealth OR Title with : Asset Servicing OR Title with : Assistant Analyst OR Title with : Assistant Archivist OR Title with : Assistant Business Analyst OR Title with : Assistant Buyer OR Title with : Buyer OR Title with : Assistant Cat Risk Analyst OR Title with : Assistant Category Manager - Security OR Title with : Assistant Chief Information Officer OR Title with : Assistant Chief Officer OR Title with : Assistant Compliance Officer OR Title with : Assistant Data Scientist - Commercial Insurance OR Title with : Assistant Director - Contracts And Delivery Assura OR Title with : Assistant Director Of Analytics OR Title with : Assistant Director Security & Justice Sector Focus OR Title with : Assistant Duty Manager - Security OR Title with : Assistant Manager - Ftc OR Title with : Assistant Manager- Logistics & Security OR Title with :

Assistant Manager Risk OR Title with : Assistant Manager Security - Old Bond Street OR Title with : Assistant Planner OR Title with : Assistant Planning OR Title with : Assistant Privacy Officer OR Title with : Assistant Production OR Title with : Assistant Professor In Biology OR Title with : Assistant Professor In Social Science OR Title with : Assistant Quality Manager OR Title with : Assistant Relationship Manager OR Title with : Assistant Security And Operations Manager OR Title with : Assistant Security Design Consultant OR Title with : Assistant Security Engineer OR Title with : Assistant Security Event Manager OR Title with : Assistant Security Manager OR Title with : Assistant Security Officer OR Title with : Assistant Site Manager OR Title with : Assistant Solutions Delivery Manager OR Title with : Assistant Support Engineer OR Title with : Assistant Team Manager OR Title with : Assistant To A Security Systems Consultant And Design Manager OR Title with : Assistant Warehouse Manager OR Title with : Assistant Workshop Supervisor OR Title with : Assistant/Paralegal OR Title with : Associate - Client Service OR Title with : Associate - Energy And Infrastructure OR Title with : Associate - Family OR Title with : Associate - Multiple Roles OR Title with : Associate | It/Data Protection OR Title with : Associate A Client Service OR Title with : Associate Audit Director OR Title with : Associate Client Service Support OR Title with : Associate Compliance And Membership Specialist OR Title with : Associate Director, Business, Strategy And Operations OR Title with : Associate I OR Title with : Associate II OR Title with : Associate Junior - Data Protection OR Title with : Associate Junior-Level - Data Protection OR Title with : Associate Nexus - Multiple Roles OR Title with : Associate Project Manager OR Title with : Associate Risk Officer Quantitative Analyst OR Title with : Associate Security Tutor OR Title with : Associate, Reporting And Analytics Multiple Roles OR Title with : Astrophysics OR Title with : At&T Senior OR Title with : Attendance Centre OR Title with : Attorney OR Title with : Audio OR Title with : Audit & Governance Officer OR Title with : Audit & Risk Lead OR Title with : Audit And Quality Specialist OR Title with : Audit and Risk Senior Analyst OR Title with : Audit Assistant OR Title with : Audit Compliance Officer OR Title with : Audit Coordinator OR Title with : Audit Manager - Data Analytics OR Title with : Audit Manager, Data Analytics OR Title with : Audit Manager, Electronic Trading OR Title with : Audit Manager,Data Analytics OR Title with : Audit Manager,Electronic Trading OR Title with : Audit Risk And Control Analyst OR Title with : Audit Senior OR Title with : Audit Supervisor OR Title with : Audit Support OR Title with : Audit Team Leader OR Title with : Auditing Manager OR Title with : Audit Manager OR Title with : Bank Network Specialist OR Title with : Banking OR Title with : Basel Risk OR Title with : Behavioural OR Title with : Bench Operative OR Title with : benchmark OR Title with : benefits OR Title with : berater OR Title with : BI OR Title with : bia data OR Title with : Bid OR Title with : Billing Assistant OR Title with : BIM OR Title with : Biomedical OR Title with : Biometrics OR Title with : Biotechnologist OR Title with : Black Rod OR Title with : Body Worn OR Title with : Bodyshop OR Title with : Boiler OR Title with : Booker OR Title with : Bookkeeper OR Title with : Border Security OR Title with : Bowe Fusion OR Title with : brand OR Title with : branding OR Title with : broker OR Title with : broking OR Title with : building OR Title with : bureau OR Title with : buried network OR Title with : bus analyst OR Title with : bus chaperone OR Title with : bus part OR Title with : Business & Operations Manager OR Title with : Business Administation Apprentice OR Title with : Business Administration Apprentice OR Title with : Business Analyst - Client Servicing OR Title with : Business Analyst - Conduct Risk OR Title with : Business Analyst - Contract OR Title with : Business Analyst - Risk OR Title with : Business Analytics Senior Manager Individual OR Title with : Business Associate OR Title with : Business Case OR Title with : Business Change OR Title with : Business Communications OR Title with : Business Deal OR Title with : Business Development OR Title with : Business Devlopment OR Title with : Business Engagement OR Title with : Business Hunter OR Title with : Business Improvement OR Title with : Business Manager OR Title with : Business Navigator OR Title with : Business Office Consultant OR Title with : Business Operational Manager OR Title with : Business Relationships OR Title with : Business Relationship OR Title with : Business Transformation OR Title with : Business Support OR Title with : Business Travel OR Title with : Buying OR Title with : CAD Technician OR Title with : CAFM OR Title with : Calculation OR Title with : Calculations OR Title with : Call OR Title with : Calling OR Title with : Campaign OR Title with : campus OR Title with : canteen OR Title with : capital OR Title with : Cardiac OR Title with : Cards Credit OR Title with : Credit OR Title with : Care OR Title with : careers OR Title with : carer OR Title with : carers OR Title with : Caretaker OR Title with : Carpenter OR Title with : CASB OR Title with : case OR Title with : Cashier OR Title with : Cashroom OR Title with : CASS OR Title with : Casual OR Title with : Catastrophe OR Title with : Category OR Title with : Catering OR Title with : CDD, Quality OR Title with : Central Compliance OR Title with : Central Control OR Title with : Central Controls OR Title with : Centre of Planning OR Title with : Change Project Manager OR Title with : Change Risk OR Title with : Channel Executive OR Title with : Channel Manager OR Title with : Channel Partner OR Title with : Chartered Surveyor OR Title with : Check In OR Title with : Chef OR Title with : Chemist OR Title with : Chief Executive OR Title with : Chief Financial Officer OR Title with : child OR Title with : citizen OR Title with : children OR Title with : Civil Engineer OR Title with : Civil Infrastructure OR Title with : civil/senior OR Title with : civils OR Title with : Claim OR Title with : Claimant OR Title with : Claims OR Title with : Classified Document Registrar OR Title with : Classroom OR Title with : Cleaner OR Title with : clean air OR Title with : Cleaning OR Title with : clearing OR Title with : Clerical OR Title with : clerk OR Title with : Client OR Title with : Climate OR Title with : clinical OR Title with : CLO Analyst OR Title with : Coach OR Title with : Commercial OR Title with : commodities OR Title with : commodity OR Title with : comms OR Title with : communication OR Title with : communications OR Title with : compensation OR Title with : Competitive OR Title with : Complaints OR Title with : Compl Risk OR Title with : Completions OR Title with : Complex OR Title with : Compliance Risk OR Title with : Concierge OR Title with : Conduct Risk OR Title with : Confectionary OR Title with : Conference OR Title with : Conflict, Security & Violence OR Title with : Conflicts OR Title with : Construction OR Title with : Consultancy - Credit & Risk OR Title with : contact centre OR Title with : Contact Centre Agent OR Title with : content editor OR Title with : content manager OR Title with : Contract Digitisation OR Title with : Control Analyst OR Title with : cookery OR Title with : Copper Jointing OR Title with : Corporate OR Title with : Financing OR Title with : Finance OR Title with : PMO OR Title with : Tax OR Title with : Correspondence OR Title with : cost OR Title with : counsel OR Title with : legal OR Title with : Counterparty OR Title with : Credit Risk OR Title with : Country Manager OR Title with : Country Risk OR Title with : Country Risk Analyst OR Title with : Country Security OR Title with : Creative OR Title with : Crematorium OR Title with : Crime & Security Manager OR Title with : crime manager OR Title with : Criminal Data OR Title with : crispr OR Title with : CRM OR Title with : Cross-Border Data OR Title with : Crude Risk OR Title with : Current Vacancies OR Title with : Customer Experience OR Title with : Customer Risk OR Title with : Data - Bi OR Title with : Data & Analytics OR Title with : Data & Bi OR Title with : Data & Mi OR Title with : Data & Operations OR Title with : Data & Performance OR Title with : Data Analyst - Risk OR Title with : Data Entry OR Title with : Deal Desk Analyst OR Title with : Debt OR Title with : Dealer OR Title with : Defect OR Title with : Defendant OR Title with : Deliveroo OR Title with : Demand OR Title with : Demonstration, Website And Event Assistant OR Title with : Depot OR Title with : Deputy Team Manager OR Title with : Derivative OR Title with : derivatives OR Title with : dermatologist OR Title with : Despatch Controller OR Title with : Detainee Custody Manager - Security OR Title with : Digital Analytics OR Title with : Recruiter OR Title with : Recruitment OR Title with : Directorate Security Manager OR Title with : Disability OR Title with : Disabled OR Title with : Disclosure Officer OR Title with : Dispatch OR Title with : dispenser OR Title with : Dividend Event Reconciliation Analyst OR Title with : Domestic OR Title with : Door OR Title with : DP OR Title with : Drainage OR Title with : Drilling OR Title with : Driver OR Title with : DRP OR Title with : due diligence OR Title with : Duty OR Title with : EAC OR Title with : Early Help OR Title with : Ebs OR Title with : EC & i OR Title with : EC&I OR Title with : eco systems OR Title with : E-commerce OR Title with : Economic OR Title with : Economics OR Title with : Elearning OR Title with : E-Learning OR Title with : Electrician OR Title with : electronic OR Title with : electromechanical OR Title with :

electronics OR Title with : event OR Title with : emergency OR Title with : employability OR Title with : employee OR Title with : employer OR Title with : HR OR Title with : Human Resources OR Title with : Energy OR Title with : empowerment OR Title with : enforcement OR Title with : engine OR Title with : enterprise OR Title with : environment OR Title with : environmental OR Title with : epidemiology OR Title with : equity OR Title with : equities OR Title with : escort OR Title with : estate OR Title with : estates OR Title with : estimating OR Title with : estimator OR Title with : facilities OR Title with : farm OR Title with : fault OR Title with : field OR Title with : financial OR Title with : finances OR Title with : fixed OR Title with : flood OR Title with : waste OR Title with : foreman OR Title with : forklift OR Title with : fostering OR Title with : fraud OR Title with : front of house OR Title with : fund OR Title with : funding OR Title with : fundraising OR Title with : fx OR Title with : gate OR Title with : general manager OR Title with : gates OR Title with : genetics OR Title with : genomics OR Title with : geospatial OR Title with : geographic OR Title with : GIS OR Title with : Global OR Title with : goods OR Title with : GRC OR Title with : Group OR Title with : growth OR Title with : headhunter OR Title with : health OR Title with : heat OR Title with : help OR Title with : helpline OR Title with : helpdesk OR Title with : high risk OR Title with : highway OR Title with : highways OR Title with : horticulture OR Title with : hospice OR Title with : hospitality OR Title with : host OR Title with : hotel OR Title with : house of commons OR Title with : housing OR Title with : humanitarian OR Title with : immigration OR Title with : Independence Support OR Title with : India OR Title with : Information Officer OR Title with : Insight OR Title with : install engineer OR Title with : Insurance OR Title with : Investment OR Title with : KYC OR Title with : Laboratory OR Title with : labourer OR Title with : land OR Title with : large format OR Title with : law OR Title with : LAYWER OR Title with : solicitor OR Title with : compliance OR Title with : Contract OR Title with : Technician OR Title with : licensing OR Title with : life sciences OR Title with : liquidity OR Title with : litigation OR Title with : loan OR Title with : loans OR Title with : locality OR Title with : locksmith OR Title with : locum OR Title with : logistics OR Title with : machine OR Title with : magic OR Title with : maintenance OR Title with : mail OR Title with : mailing OR Title with : major works OR Title with : mammographer OR Title with : management information OR Title with : Manager in Policing OR Title with : Market Risk OR Title with : Marketing OR Title with : marketplace OR Title with : markets OR Title with : master data OR Title with : mechanical OR Title with : media OR Title with : medical OR Title with : mental OR Title with : mentor OR Title with : Metocean Risk OR Title with : Mi OR Title with : Micro OR Title with : microscopy OR Title with : midday OR Title with : middle OR Title with : Model RISK OR Title with : Molecular OR Title with : money OR Title with : mortality OR Title with : mortgage OR Title with : policy OR Title with : nurse OR Title with : nursing OR Title with : nursery OR Title with : Occupational OR Title with : Office Assistant OR Title with : Office Consultant OR Title with : Office Junior OR Title with : office manager OR Title with : office supervisor OR Title with : onboarding OR Title with : Operational Risk OR Title with : Operations Manager OR Title with : Operations Officer OR Title with : Order Processing OR Title with : Organisation OR Title with : organisational change OR Title with : P Specialist OR Title with : P&L OR Title with : PA OR Title with : Package Manager OR Title with : Paint OR Title with : Painter OR Title with : Painting OR Title with : Panel OR Title with : Paraplanner OR Title with : parking OR Title with : Parliamentary OR Title with : Part Qualified OR Title with : participation OR Title with : Passenger OR Title with : Pathology OR Title with : Patient OR Title with : Payment Advisor OR Title with : Payroll OR Title with : Reconciliation OR Title with : PB Analytics OR Title with : Pension OR Title with : pensions OR Title with : People OR Title with : Performance OR Title with : performer OR Title with : perinatal OR Title with : Peripatetic OR Title with : Personal Assistant OR Title with : Personnel OR Title with : pharmacist OR Title with : pharmaceuticals OR Title with : Pharmacology OR Title with : Pharmacy OR Title with : photocopier OR Title with : physicist OR Title with : Physiology OR Title with : Physiotherapist OR Title with : physiotherapy OR Title with : picking OR Title with : pilot OR Title with : planner OR Title with : plumber OR Title with : plumbing OR Title with : podiatry OR Title with : political OR Title with : port OR Title with : porter OR Title with : portfolio OR Title with : pricing OR Title with : process OR Title with : procurement OR Title with : production OR Title with : programmes OR Title with : property OR Title with : proposal OR Title with : psychiatrist OR Title with : provisioning OR Title with : Public Affairs OR Title with : Public Relations OR Title with : purchase ledger OR Title with : QS OR Title with : quality OR Title with : quantitative OR Title with : quantity OR Title with : Radiographer OR Title with : radiographic OR Title with : rail OR Title with : reception OR Title with : records OR Title with : refrigeration OR Title with : regeneration OR Title with : regional OR Title with : registration OR Title with : regulation OR Title with : Regulatory OR Title with : relationship OR Title with : relief OR Title with : relocate OR Title with : remedial OR Title with : remediation OR Title with : renewals OR Title with : rent OR Title with : repair OR Title with : Reports Consultant OR Title with : Reserving OR Title with : Resident Engineer OR Title with : Residential OR Title with : Resourcing OR Title with : response engineer OR Title with : restaurant OR Title with : retail OR Title with : Retirement OR Title with : revenue OR Title with : revenues OR Title with : review analyst OR Title with : Rights Officer OR Title with : reward OR Title with : risk- OR Title with : risk & OR Title with : risk and OR Title with : Risk and Econometrics OR Title with : install OR Title with : secretary OR Title with : installation OR Title with : predictive modelling OR Title with : shift OR Title with : share OR Title with : social media OR Title with : social research OR Title with : sourcing OR Title with : medicine OR Title with : speech OR Title with : sports OR Title with : staffing OR Title with : stage OR Title with : stakeholder OR Title with : stalking OR Title with : statistician OR Title with : stock OR Title with : store OR Title with : student OR Title with : strategic OR Title with : structural OR Title with : street OR Title with : submarine OR Title with : supervisory OR Title with : supplier OR Title with : supply OR Title with : support officer OR Title with : support administrator OR Title with : surgery OR Title with : surveyor OR Title with : tableau OR Title with : switchboard OR Title with : swaps OR Title with : teacher OR Title with : teaching OR Title with : team manager OR Title with : team leader OR Title with : team coordinator OR Title with : team assistant OR Title with : Technology Controls OR Title with : Theatre OR Title with : Third Party Risk OR Title with : therapist OR Title with : time tracking OR Title with : tracking OR Title with : trade OR Title with : Traded Credit OR Title with : Traded Risk OR Title with : trader OR Title with : trading OR Title with : training OR Title with : transaction OR Title with : transactional OR Title with : transfers OR Title with : transition OR Title with : Transport OR Title with : trauma OR Title with : travel OR Title with : treasury OR Title with : treasury/risk OR Title with : Trustee OR Title with : tutor OR Title with : licencing OR Title with : typist OR Title with : Underwriter OR Title with : underwriting OR Title with : Uniformed Security Manager OR Title with : unum OR Title with : upholsterer OR Title with : ups engineer OR Title with : urban livelihoods OR Title with : urgent care OR Title with : user acceptable OR Title with : user experience OR Title with : user research OR Title with : UX OR Title with : Valuation OR Title with : Value OR Title with : vehicle OR Title with : vendor OR Title with : venue OR Title with : vetting OR Title with : VR OR Title with : Waiting OR Title with : waiter OR Title with : water OR Title with : wealth OR Title with : young OR Title with : social worker OR Title with : psychology

# Our standards and accreditations

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

## ISO 20252

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

## Market Research Society (MRS) Company Partnership

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

## ISO 9001

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

## ISO 27001

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

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

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

## HMG Cyber Essentials

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

## Fair Data

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

# For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

**www.ipsos-mori.com**
**http://twitter.com/IpsosMORI**

## About Ipsos MORI Public Affairs

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