Cyber security skills in the UK labour market 2022

Technical report

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

Department for Digital, Culture, Media & Sport

Ipsos

Contents

1 Overview

The UK government Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos and Perspective Economics to conduct the latest in an annual series of studies to improve their understanding of the current UK cyber security skills labour market. The previous studies were published by DCMS in 2021 (fieldwork in 2020), 2020 (fieldwork in 2019) and 2018.

This report provides the technical details for all strands of the 2022 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.

1.1 Full research objectives

The 2022 research, in line with previous years, aimed to gather evidence on:

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

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

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

1.2 Summary of methodology

The methodology consisted of 4 strands:

1. **Quantitative surveys** – Ipsos conducted representative telephone surveys with 4 audiences: general businesses, public sector organisations, charities and cyber sector firms. These surveys gathered the main estimates on skills gaps and shortages reported in this study. Fieldwork was between 16 August and 19 November 2021.

2. **Qualitative interviews** – Ipsos conducted a more focused strand of qualitative research, with 29 in-depth interviews split across cyber firms, other medium and large businesses, and recruitment agents. The interviews explored the challenges these organisations faced in addressing skills gaps and shortages, and the approaches they were taking on recruitment, training and workplace diversity. Interviews took place across October and November 2021.

3. **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Burning Glass Technologies labour market database, showing the number, type and location of vacancies across the UK. This also covers remuneration, descriptions of job roles and the skills, qualifications and experience being sought by employers. This work primarily covered vacancies across the 12 months of 2021, supplementing the work done in the 2021 study (which covered vacancies from September 2019 to the end of December 2020).

4. **Supply side analysis** – Perspective Economics replicated the methodology used on the 2021 cyber recruitment pool research to estimate the overall size of the current recruitment pool, as well as those likely to be entering the pool within the next 12 months (across 2022). This strand produces further statistics on the diversity, educational and occupational backgrounds, and salaries of this pool of labour, as well as outflows from the pool.

1.3 Similarities and differences from the 2021 study

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

Questionnaire changes

The quantitative survey questions are reviewed and partially revised each year to ensure we capture the metrics that are most useful for DCMS and its stakeholders. This year, we included new questions to break down the cyber workforce by specialism and to categorise the hard-to-fill vacancies that cyber sector businesses face. To make space for these questions, we removed questions from the previous surveys. The rationale for these changes 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).

New fieldwork measures to counter the COVID-19 pandemic

This year's survey fieldwork was once again heavily impacted by the COVID-19 pandemic. Many organisations were less able or willing to take part in government surveys in general, compared to typical pre-pandemic expectations for a survey of this nature. Many organisations also continue to not be contactable by phone, especially when it comes to reaching back-office staff in IT or cyber security roles.

Having anticipated this challenge, Ipsos implemented a range of measures this year to help improve the survey sample coverage and response rate, including:

- Additional number matching, as well as matching in relevant contact names and emails – see Chapter 2 for more details
- Multimode surveying, allowing respondents to take part either by telephone or online – see Chapter 2 for more details
- A series of prompt emails to the sample (where an email address was available)
- A freephone number and survey inbox for sampled organisations to opt in, either to take part immediately or arrange an appointment
- Promotion of the survey to the cyber sector via Cyber Exchange, the Cyber Security Clusters and TechUK

We do not expect these measures to affect the comparability of the survey between years.

Despite these measures, the considerable ongoing challenges caused by the COVID-19 pandemic ultimately meant that response rates this year were similar to those from the previous year, rather than an improvement on them. We discuss in Section 2.4. We do not expect this to have had any major detrimental impact on the reliability of the findings.

Sample sizes

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

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

The margin of error for the overall business sample is broadly in line with last year, at ±3-4 percentage points.[1] As expected, the margin of error has decreased for large businesses (from ±8-13 percentage points in 2021 to ±6-10 percentage points in 2022), public sector organisations (from ±7-12 points to ±5-9 points) and cyber firms (from ±4-7 points to ±4-6 points).

Recommendations

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

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

1.4 Differences from other recent studies looking at cyber security skills

A note on the UK cyber security workforce size estimate from the 2021 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 2021. This is a study of the global cyber security workforce and largely reports its findings at a global level.

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

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

DCMS's Cyber Sectoral Analysis 2022 estimates c.53,000 full-time employees working in cyber roles in the UK cyber sector, across the 1,838 cyber security companies that make up this sector. This excludes individuals working in cyber roles outside of these companies.

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

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

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

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

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

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

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

1.5 Acknowledgements

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

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

2 Quantitative surveys

Ipsos 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 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).

A significant change this year was updating the entire questionnaire to work as a multimode telephone and online survey script – this is covered further in Section 2.4. Besides this, there were minimal changes in the questionnaire this year, compared to the previous iteration. The minor changes reflected new areas that DCMS wished to gain further statistical information on, including:

- A new question to break down the cyber sector workforce by specialism (Q18d/e)
- Updating the list of job roles in the question classifying hard-to-fill vacancies (Q46b) to reflect the same specialisms used in the aforementioned new question
- Updating the term “soft skills” to “complementary skills”, reflecting how DCMS refers to this (Q28)

The change to Q46b moved the question away from an older list aligned to the Chartered Institute of Information Security (CIISec) Roles Framework. It replaced it with an updated list that better reflected DCMS’s categorisation of job roles and aligned to the work of the UK Cyber Security Council and the Cyber Security Body Of Knowledge (CyBOK). This change is significant, and this question is no longer comparable with previous years.

The change to Q28 is more minor, and we still consider this question to be comparable to 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 2021, as part of the Cyber Sectoral Analysis 2022. 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.

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 approved their exclusion, in line with previous years, given the additional permission needed to sample these organisations from the IDBR.

In total, we selected 56,159 businesses and public sector organisations from the IDBR. This is similar to the total number we requested last year (60,500). It was more than in 2020 (48,702) and 2018 (37,871), anticipating that the ongoing COVID-19 pandemic would continue to make fieldwork more challenging and a larger sample would be required to reach targets.

We selected records 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 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 series)

Table 2.1 breaks down the originally selected sample by size and sector. As the survey outcomes later in this chapter show, only 12,568 IDBR records were included in the final survey, with the rest being unusable (i.e. with no valid telephone number) or being held in reserve.

Table 2.1: Pre-cleaning IDBR sample received 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)	770	234	1,494	2,498
F	Construction	5,663	114	303	6,080
G	Retail or wholesale (including vehicle sales and repairs)	2,836	313	1,196	4,345
H	Transport or storage	2,366	86	410	2,862
I	Food or hospitality	4,113	171	612	4,896
J	Information or communications	7,575	641	433	8,649
K	Finance or insurance	1,924	498	404	2,826
L, N	Administration or real estate	5,242	165	1,288	6,695
M	Professional, scientific or technical	4,292	203	755	5,250
O	Other public sector	341	168	444	953
P	Education (including academies)	2,018	571	1,001	3,590

SIC 2007 letter	Sector description	Micro or small (1–49 staff)	Medium (50–249 staff)	Large (250+ staff)	Total
Q	Health, social care or social work (including NHS)	4,264	272	778	5,314
R, S	Entertainment, service or membership organisations	1,870	45	286	2,201
	Total	43,274	3,481	9,404	56,159

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 all the previous studies.

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.

Once again 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 211 (vs. 220 in 2021, 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 1,064 charities to achieve 211 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 2022 (also carried out by Ipsos and Perspective Economics). Perspective Economics built this sample frame, a list of 1,624 UK cyber sector firms, from the Orbis and Beauhurst databases. From this database, there were 1,507 records with telephone numbers.

All 1,507 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 224 interviews.

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

Not all the original sample was usable. In total, 42,129 business records 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) in the original sample file.

This year, as part of a raft of measures to improve telephone coverage and response rates, we carried out a more extensive programme of telephone matching. We carried out automated telephone matching through the DBS Data business database as well as the Dun and Bradstreet business database. In previous years, we have matched to the DBS Data residential database for micro businesses. However, this is no longer possible due to data protection and ethical concerns around attempting to survey business respondents via a database consisting largely of consumer numbers.

In addition to matching telephone numbers, we also matched in email addresses (generic email addresses as well as those for key decision makers) and key decision maker contact names where possible. These were sourced from the Dun and Bradstreet database, public LinkedIn data, Companies House data and other publicly accessible data (e.g. company websites). These details were subsequently used for prompt emails to the loaded sample and to help bypass gatekeepers (by giving the name of a specific individual within the business).

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 2021, as part of DCMS's Cyber Sectoral Analysis 2022. However, we did a subsequent manual search for missing cyber sector numbers on company websites. Across the IDBR and cyber sector samples, these processes increased the amount of usable sample, helping 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 (99% 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 22,811 leads. This is 39 per cent of the original sample frame, compared to 24 per cent in 2021, highlighting the impact of the process to improve telephone coverage. The composition of this sample is shown in Table 2.2.

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)	362	224	1,315	1,901
F	Construction	1,444	103	256	1,803
G	Retail or wholesale (including vehicle sales and repairs)	1,150	285	1,026	2,461
H	Transport or storage	374	80	354	808
I	Food or hospitality	1,497	136	499	2,132
J	Information or communications	1,353	504	325	2,182
K	Finance or insurance	1,184	425	338	1,947
L, N	Administration or real estate	1,310	139	1,091	2,540
M	Professional, scientific or technical	988	179	562	1,729
O	Other public sector	56	132	335	523
P	Education (including academies)	662	355	723	1,740
Q	Health, social care or social work (including NHS)	1,183	250	636	2,069
R, S	Entertainment, service or membership organisations	714	33	229	976
	Total	12,277	2,845	7,689	22,811

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 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).

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 (16-17 August 2021). 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 35 live pilot telephone interviews among the four audiences for the study (24 charities and 11 cyber sector businesses). Due to delays in receiving and processing the IDBR sample from the Office for National Statistics (ONS), this was launched after the pilot this year.

Following the live pilot, we only made minor changes to the questionnaire. The main change involved adding an unprompted “not applicable – no devices belonging to organisation” code to Q29 and Q34 – questions about detecting malware on the organisation’s devices – following feedback from interviewers.

These 35 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

Multimode data collection

As part of a range of measures this year to help improve the survey sample coverage and response rate during the COVID-19 pandemic, we implemented multimode surveying, allowing respondents to take part either by telephone or online. This was in place for the live pilot and main fieldwork (although all live pilot interviews were by telephone). The previous years' surveys were conducted by telephone only.

In practical terms, the multimode methodology worked as follows:

- All initial contact with organisations took place by phone, with Ipsos telephone interviewers calling organisations in line with previous years
- Where organisations requested more information before deciding to take part, interviewers could send out an information and reassurance email. This email contained a unique link for each organisation to complete the survey entirely or partially online. The interviewers explained this ahead of sending out each email
- The respondents that completed the survey online had no interaction with an Ipsos interviewer but were instead routed through an online questionnaire, with each question appearing on a separate screen
- Over the course of fieldwork, we sent 2 reminder emails to those that had started but not finished the survey online

Table 2.3 shows that around 4% of the achieved interviews in total were online. In other words, the overwhelming proportion of interviews were still by telephone.

Table 2.3: Interviews by data collection mode

Mode	Businesses		Public sector		Charities		Cyber sector		Total	
	N	%	N	%	N	%	N	%	N	%
Telephone	919	97%	108	89%	204	97%	213	95%	1,446	96%
Online	28	3%	13	11%	7	3%	11	5%	59	4%

We are aware of the potential for the change in the data collection mode to impact the survey results. If this mode effect is significant, any changes in the results compared to previous years may not reflect a real shift in the population.

DCMS and Ipsos did not expect there to be substantial mode effects in this survey, given that much of the information collected is factual, rather than attitudinal. Nevertheless, we had various measures to minimise the chances of mode effects and to monitor the data to identify mode effects:

- The intention was for only a small proportion of the sample to complete the survey online, so that any potential mode effects would be contained. In this case, we did not have to cap the number of online interviews, given that it was only 4 per cent of all completed interviews
- We used unimode questionnaire design wherever feasible, whereby the questionnaire administration is as similar as possible for respondents across modes. For example, sequential statements on the telephone survey (e.g. at Q13.WHATOUT) appear as a carousel of statements in the online survey. We minimised the number of questions with long, unprompted answer lists in

the telephone survey (which would need to be prompted answer lists in the online survey), such as Q44.OTHRECRUIT, Q47.HARDREASON and Q47e.REASON

- We added a screener question to the online survey (Q1x.ONLINERESP) for respondents to self-validate that they were the right person within their organisation to complete the survey – something the telephone interviewer would have established verbally. This was an extra quality assurance to prevent the survey being completed by someone who would be unable to answer many questions
- As part of the final data checks, we manually reviewed the answers of online respondents to see if they followed a pattern that was substantially different from telephone respondents in the same sample group, or if they included a long string of "don't know" responses. Following these broad checks, we did not need to remove any online respondents from the final data

Completed interviews

All survey fieldwork (including the live pilot) was carried out from 16 August to 19 November 2021. This included a fieldwork extension of 3 weeks compared to the original timetable to counteract the impact that the COVID-19 pandemic was having on participation. This is explained further in the response rate section (at the end of Section 2.4).

In total, we completed 1,505 interviews, comprising:

- 947 businesses (excluding agriculture, forestry and fishing businesses and sole traders)
- 123 public sector organisations (excluding parish councils)
- 211 registered charities
- 224 cyber sector businesses

The average interview length was c.16 minutes for businesses, public sector organisations and charities and c.17 minutes for cyber firms.

Fieldwork preparation

Prior to fieldwork, the Ipsos 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 organisation was eligible for the survey. At this point, organisations *outside* the cyber sector that identified themselves as sole traders with no other employees on the payroll would have been classed as ineligible. *Within* the cyber sector, sole trader cyber firms were still eligible, in line with previous years, because this survey still intended to capture the skill, training and recruitment needs of the firm's founder.

In previous years, organisations that identified themselves as having no computer, website or other online presence were also classed as ineligible. Last year, this accounted for around 1 per cent of the businesses and 4 per cent of the charities sampled. This year, this classification was removed as part of a simplification of call outcomes. Organisations saying this were, in all likelihood, simply refusing to take part. This partially helps to explain the higher refusal rate this year, covered in Section 2.4.

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.

Organisations sampled from the IDBR were able to self-identify as a registered charity during the interview. In these cases, they were included in the charity sample data. They are part of the response rate calculation for the charity sample.

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 the previous iterations of this research:

- 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 judgement 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 to encourage participation.

Additional steps taken in light of the COVID-19 pandemic

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

- Additional number matching – we matched to 2 databases this year (as noted in Section 2.2) and undertook further manual matching (i.e. looking up numbers on company websites) for cyber firms
- Adding key decision maker contact names to the matched sample where possible (as noted in Section 2.2) to help interviewers get past gatekeepers and organisation no-name policies
- Multimode surveying (as noted at the start of this section)
- Adding email addresses to the matched sample where possible – we sent advance emails to new batches of sample loaded, alerting them that an Ipsos interviewer would call and encouraging them to book an appointment, as well as 5 sets of reminder emails to loaded sample across the course of fieldwork (each with a varied subject heading and key message). In total, 41 per cent of the released sample had an email address, although these were largely general information or enquiries email addresses for the organisation as a whole
- 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
- Promotion of the survey to the cyber sector via Cyber Exchange, the Cyber Security Clusters and TechUK – we created a promotional deck explaining the survey that DCMS and Ipsos sent to these organisations for them to distribute among their members

Fieldwork monitoring

Ipsos 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 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 research team monitored fieldwork outcomes and response rates throughout fieldwork and gave interviewers regular guidance on how to avoid common reasons for refusal. Table 2.4 shows the final outcomes, the unadjusted response rate[2] and the adjusted response rate[3] for business and public sector (the IDBR sample). Tables 2.5 and 2.6 show the equivalent for charities and cyber firms.

Table 2.4: Fieldwork outcomes and response rate calculations for businesses and public organisations (IDBR sample)

Outcome	Total
Total sample released	12,568
Completed interviews	1,070
Incomplete interviews	98
Ineligible leads – established during screener[4]	194
Refusals	1,844
Unusable leads with working numbers[5]	1,811

[2] This is: completed interviews / total sample released.
[3] The adjusted response rate with estimated eligibility has been calculated as: completed interviews / (completed interviews + incomplete interviews + refusals expected to be eligible + any remaining working numbers expected to be eligible). It adjusts to exclude the unusable and likely ineligible proportion of the total sample used.
[4] Among the IDBR and charity samples, ineligible leads were those found to be sole traders. Among the cyber sector sample, this included a small number of firms that did not recognise themselves to be firms offering cyber products or services.
[5] 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.

Outcome	Total
Unusable numbers[6]	747
Working numbers with unknown eligibility[7]	6,804
Expected eligibility of screened respondents[8]	86%
Unadjusted response rate	9%
Adjusted response rate	12%

Table 2.5: Fieldwork outcomes and response rate calculations for charities

Outcome	Total
Total sample released	1,064
Completed interviews	211
Incomplete interviews	17
Ineligible leads – established during screener	14
Refusals	105
Unusable leads with working numbers	123
Unusable numbers	75
Working numbers with unknown eligibility	5194
Expected eligibility of screened respondents	94%
Unadjusted response rate	20%
Adjusted response rate	26%

Table 2.6: Fieldwork outcomes and response rate calculations for cyber firms

Outcome	Total
Total sample released	1,502
Completed interviews	224
Incomplete interviews	12
Ineligible leads – established during screener	4
Refusals	240
Unusable leads with working numbers	387
Unusable numbers	111
Working numbers with unknown eligibility	524
Expected eligibility of screened respondents	98%
Unadjusted response rate	15%
Adjusted response rate	23%

[6] 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.
[7] 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.
[8] 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 and working numbers expected to have been eligible for the survey.

Unadjusted response rates compared to previous years

Compared to last year, the unadjusted response rate (URR) for the IDBR sample is identical (9% in both years). For charities, the URR is higher this year (20% vs. 15%). Finally, for cyber firms, the URR is lower this year (15% vs. 18%). Therefore, the survey has performed broadly in line with last year across all groups.

However, when compared to previous years, the URRs are lower for the IDBR sample (11% in 2020 and 14% in 2018), charities (36% in 2020 and 30% in 2018) and cyber firms (22% in 2020, when this population was first surveyed for this series).

The lower URRs compared to the pre-pandemic surveys are likely to be due to a combination of unique circumstances brought about by COVID-19, as well as the ongoing challenge of declining response rates in social survey fieldwork in general (see, for example, this Government Statistical Service blog on declining response rates). This survey's fieldwork took place when many organisations were adopting either full remote working or a hybrid working model, where cyber teams would not necessarily be in offices across the working week. More than half the fieldwork also took place before the end of the government's Coronavirus Job Retention Scheme, through which employers could furlough workers. The environment under which fieldwork took place meant:

- It was harder to reach organisations via landline numbers as many switchboards still 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
- 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.

Adjusted response rates compared to previous years

The adjusted response rate (ARR) adjusts to exclude the unusable and likely ineligible proportion of the total sample used. This year's ARRs should not be directly compared to the ARRs published in previous years' technical reports. We have simplified the ARR calculation this year to use a single percentage figure for estimated eligibility, applied to both the refusals and the working numbers with unknown eligibility. For retrospective comparison, if we had calculated response rates in this way last year, the ARRs would have been as follows – broadly meeting or exceeding last year's ARRs:

- 13 per cent for the IDBR sample in 2021, vs. 12 per cent this year
- 21 per cent for charities, vs. 26 per cent this year
- 21 per cent for cyber firms, vs. 23 per cent this year

Expected negligible impact of lower response rates compared to pre-pandemic

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.[9]

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 the COVID-19 pandemic, then we must consider whether the organisations most negatively impacted by COVID-19 are likely to have different cyber skills needs and challenges – we have no strong reasons to believe this. It is possible that COVID-19 and the resulting move to hybrid working in many organisations has presented its own set of cyber skills challenges, which we aim to capture separately in the qualitative strand of the research.

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[10]), 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’ 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 research team, who checked and approved each new code proposed.

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.[11] 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

[9] 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).

[10] The definitions for these SIC letters is in Table 4.1.

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

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).[12] 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:

- 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 2022 survey, which was also not weighted. This is the best comparison to indicate whether the sample is skewed in any way, given that it uses the same sample frame and methodology as this survey, and enables us to benchmark the achieved profile against several previous years of data. 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.

[12] Ahead of the publication of this report, more recent BEIS (2021) business population estimates have been published. We opted not to reweight our data with these updated statistics, as the population profile was not notably different from the previous year. Reweighting would have had a negligible impact on the survey data.

Table 2.7: 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)	73%	97%
Medium (49–249 staff)	16%	3%
Large (250+ staff)	11%	1%
Sector		
Administration or real estate	10%	13%
Construction	7%	13%
Entertainment, service or membership organisations	4%	7%
Finance or insurance	9%	2%
Food or hospitality	7%	10%
Information or communications	8%	6%
Professional, scientific or technical	8%	14%
Retail or wholesale	12%	18%
Transport or storage	3%	4%
Utilities or production (including manufacturing)	6%	7%
Region		
East Midlands	6%	6%
Eastern	9%	9%
London	18%	18%
North East	3%	3%
North West	9%	9%
Northern Ireland	3%	3%
Scotland	7%	7%
South East	15%	15%
South West	11%	11%
Wales	3%	3%
West Midlands	9%	9%
Yorkshire and Humberside	7%	7%

Table 2.8: Unweighted and weighted sample profiles for charities

	Unweighted %	Weighted %
Income band[13]		
£0 to under £100,000	36%	78%
£100,000 to under £500,000	20%	15%
£500,000 or more	40%	8%

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

Table 2.9: 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)	28%	25%
Medium (49–249 staff)	41%	45%
Large (250+ staff)	31%	30%
Sector		
Education (including academies)	12%	2%
Health, social care or social work (including NHS)	11%	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)
- Distribution of the cyber sector workforce by specialism (Figure 2.6)
- 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.

We did not remove any outliers this year, but we have in the findings report acknowledged the substantial impact that the two large cyber firm respondents this year have on the diversity estimates. There was a similar impact in previous years – these larger firms tend to have a more diverse workforce, and their size means that this diverse workforce has a bigger impact on the overall estimates. For context, we have reported the figures both including these two large firms and excluding them (i.e. the estimate for small and medium enterprises in the cyber sector).

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 20.5%, 40.7% and 38.7%, they will show as 21%, 41% and 39%.

3 Qualitative interviews

As well as the survey, Ipsos conducted 29 qualitative in-depth interviews in October and November 2021. This included:

- 16 cyber sector businesses
- 9 medium and large organisations from other sectors (3 with 50+ staff and 6 with 250+ staff)
- 4 recruitment agents, sampled from 3 recruitment agencies, where 2 were specialists in cyber security recruitment and 2 covered recruitment for a wider range of tech roles, including cyber

The focus on larger organisations is consistent with last year's study. It 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 almost entirely recruited from the survey. In 2 cases, DCMS used their contacts to help Ipsos secure interviews with 2 large firms in the cyber sector (who subsequently took part in the survey). The sampling was purposive – Ipsos identified the best organisations to recruit based on their survey responses, with quotas applied to recruit those that had:

- Hard-to-fill job vacancies
- Externally delivered or developed training for those in cyber roles or wider staff
- Staff performing cyber functions with and without relevant qualifications in cyber security
- Taken action to improve their workforce diversity

We also applied broader quotas to ensure a mix of organisations by sector and region (and by size within the cyber sector, where recruitment was not restricted to just larger organisations).

Survey respondents gave permission to be recontacted in the survey. Our specialist recruitment team then emailed and telephoned these respondents inviting them to take part 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 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 5 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. Upon them agreeing to take part, we asked further screener questions over email, to ensure they were eligible and guide the subsequent

interview. These covered whether they recruited for specific geographic areas, particular roles or specialisms within cyber security, particular levels or grades, and any non-cyber recruitment.

For context, 2 were specialist cyber-only recruiters and 2 covered recruitment for a wide range of tech roles. All 4 recruiters typically focused on non-entry level recruitment (i.e. they did not focus on finding apprentices or graduates).

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 research team carried out each interview either over the telephone or virtually via Microsoft Teams. Each interview lasted c.60 minutes.

The topics for discussion were agreed collaboratively between Ipsos and DCMS. Ipsos 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:

- Their main challenges and gaps related to cyber security skills
- Their approaches to training, qualifications and Continuing Professional Development (CPD)
- Recruitment challenges, including hard-to-fill vacancies and assessing competencies
- Perceptions of workforce diversity and actions taken in this area
- Opinions on the Cyber Security Body Of Knowledge (CyBOK)
- Opinions on the UK Cyber Security Council's Careers Route Map

The topics covered in the recruitment agent interviews were:

- The recruitment pool, and where and how they source applicants
- The diversity of the applicant pool and cyber hiring managers' attitudes to diversity
- Employers' recruitment criteria
- Approaches to keeping up to date with industry needs
- Opinions on CyBOK
- Opinions on the UK Cyber Security Council's Careers Route Map

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 previous years' research. The new data for this year focuses on the 2021 calendar year (1 January to 31 December). The data in the previous studies has covered the period from 2016 to 2020, i.e. 4 years of data. Therefore, across both years of the study that have adopted this methodology, we have over 5 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[14] 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, 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.

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

Improving on the Burning Glass Technologies standard cyber security filter

Using the Burning Glass Technologies cyber security filter suggests that there were 153,192 cyber security job postings in the UK in 2021. 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)

For this and the previous studies, 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. Finally, we systematically 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 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).
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.

These steps have remained consistent across both the 2020 and 2021 studies.

In 2021, our revised search criteria yielded 53,144 core cyber security roles, and a further 100,048 cyber-enabled roles. In total this comes to 153,048 job postings in scope for this strand (compared to Burning Glass Technologies’ own 108,246 job postings yielded from the cyber security filter).

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

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).

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 663,000 job postings from the last c.5 years (September 2016 to December 2021 incorporating previous years' datasets), 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. 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 job sites, 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 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 Supply side analysis

Perspective Economics led this strand of the research. It replicated the methodology used on the 2021 cyber recruitment pool research to estimate the overall size of the current recruitment pool, as well as those likely to be entering the pool within the next 12 months (across 2022). In addition, this strand produces further statistics on the characteristics of the recruitment pool, in terms of:

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

5.1 Overview of metrics and data sources

Table 5.1 covers the full list of secondary data sources used in this strand and the time periods covered.

Table 5.1: Data sources for supply side analysis

Type	Metrics	Source	UK region covered	Time period covered
Further education data	▪ Number of (Degree) Apprenticeships ▪ Number of courses and students enrolled	Department for Education (DfE)	England only	2018/19 academic year (unchanged since the previous report)
Higher education data (currently enrolled students)	▪ Number of courses and higher education institutions ▪ Number of students enrolled ▪ Course titles and providers (by undergraduate and postgraduate level) ▪ Location (domicile, location of study, and location within 9 months of graduating) ▪ Demographics (gender identity, ethnicity, state school marker, age)	Higher Education Statistics Authority (HESA) and Jisc bespoke data requests, (specifically HESA Student Record data) **Cyber security related course** (agreed by Jisc, HESA and the National Cyber Security Centre, or NCSC) and **Other Computer Science** markers applied to filter data	UK-wide (England, Scotland, Wales and Northern Ireland)	2019/20 academic year

Type	Metrics	Source	UK region covered	Time period covered
Higher education data (graduate outcomes)	▪ Destination of graduates ▪ Standard Occupational Classification (SOC) 2010 and SOC 2020 ▪ Salary bands	HESA and Jisc bespoke data requests (specifically HESA Graduate Outcomes survey data) Same markers as above applied to filter data	UK-wide	2018/19 academic year (lag due to this being the most recent Graduate Outcomes survey data published)
Estimation of inflows	▪ Data on retraining, reskilling, entry from other sectors and remote working ▪ Certification data	Perspective Economics estimates based on updated certification data, where available (via CompTIA, Capslock etc.)	UK-wide	2021 estimate (certain data unchanged since the previous report)
Estimation of outflows	▪ Retirement and other reasons for leaving the cyber firm within last 12 months	Ipsos estimate based on the survey of cyber firms	UK-wide	Survey fieldwork undertaken in late 2021

The 2019/20 DfE further education and apprenticeships data was not available in time for this report. Therefore, our estimates in this area and how they feed into the estimation of inflows into the cyber security labour market are unchanged from the previous recruitment pool research. This is covered in Sections 3.3 and 3.4 of that earlier report.

The estimation of inflows from certification data and private training providers outside the state education sector are also unchanged from the previous research (see Section 3.5 of the recruitment pool report). There is no new data available to be covered for these estimates, and no expectation that this component of the inflow calculation would have substantially changed in the last year.

5.2 Cyber workforce gap calculation

The calculation of the cyber workforce gap involves the following constituent parts:

- Part A – an estimate of the additional annual demand for people in cyber security roles (beyond the current workforce)
- Part B – an estimate of inflows into the cyber security labour market (the number of new entrants into the market)
- Part C – an estimate of outflows from the cyber security labour market (the number of people exiting the market)

The calculation itself is as follows: A - B + C

The rest of this section lays out how each constituent part is calculated and the key assumptions and limitations of the calculation. The actual calculation and figures for each of the constituent parts is included in Chapter 10 of the findings report.

Part A – an estimate of the additional annual demand for people in cyber security roles

This first step in this estimation involves the creation of a midpoint estimate for the size of the current cyber security recruitment pool. We do this by creating a low-end reasonable estimate and a high-end (maximum) reasonable estimate and taking the midpoint of these 2 figures.

We have based the low-end reasonable estimate on a baseline figure for the 2016 workforce (created by the Tech Partnership in 2017).

- The previous recruitment pool research applied a 14 per cent average annual growth rate to this figure for each year up to the end of 2020, based on the growth of the cyber sector workforce as measured in successive DCMS Cyber Sectoral Analyses (published regularly since 2017)
- For estimating workforce growth from 2020 to 2021, we use the 13 per cent growth rate in the most recent Cyber Sectoral Analysis 2022

We have based the high-end (maximum) reasonable estimate on available job vacancies data from the Burning Glass Technologies database (covered in Chapter 7 of the findings report) and data on the number of full-time equivalents (FTEs) in the cyber sector (from the Cyber Sectoral Analysis 2022).

- We use job vacancies data to calculate the ratio of core cyber job roles to cyber-enabled job roles (as defined in Chapter 7 of the findings report). This is assumed to be equivalent to the ratio of cyber roles within the cyber sector to those outside the cyber sector. In other words, this ratio is assumed to tell us, for each person employed in a cyber role within the cyber sector, how many are employed in a cyber role in the wider economy
- We apply this ratio to the number of FTEs working within the cyber sector, to estimate the number of FTEs in cyber roles outside the cyber sector

We then reapply the 13 per cent growth rate in FTEs from the Cyber Sectoral Analysis 2022, to estimate the additional annual demand for 2022.

Part B – an estimate of inflows into the cyber security labour market

This is the sum of the following estimates covered in the findings report:

- The latest (2019/20) data on people graduating from higher education courses in cyber security
- The latest (2019/20) data on people graduating from higher education courses in computer science
- The latest (2018/19) data on people completing relevant further education courses – taken directly from the 2021 cyber recruitment pool research, as no new data has been published
- The latest (2018/19) data on people completing relevant apprenticeships – taken directly from the 2021 cyber recruitment pool research, as no new data has been published
- An estimation of people completing other certified training or private training courses that enable them to transition to cyber security roles (e.g. from current roles in IT) – taken directly from the 2021 cyber recruitment pool research, as we do not expect this to have significantly changed

Part C – an estimate of outflows from the cyber security labour market

We use the survey estimate of the proportion of people leaving the cyber sector (covered in Chapter 8 of the findings report) and extrapolate this to the entire cyber security workforce (within and outside the cyber sector). Applying this survey estimate to our midpoint estimate for the size of the current cyber security recruitment pool, we calculate the expected number of people who will be leaving the cyber workforce in 2022.

Key assumptions and limitations

The estimate of the workforce gap inevitably makes various assumptions, which are necessitated by the limitations of the available data:

- In calculating the size of the current cyber security recruitment pool, we create a high-end (maximum) estimate based on the number of FTEs within the cyber sector. In practice, not all the FTEs within the cyber sector are people working in cyber roles. They will also include a number of people in non-cyber roles (e.g. in diversified companies that offer cyber and non-cyber products and services), as well as administrative staff. Nevertheless, this number provides a good starting point for a high-end estimate.
- To estimate the additional annual demand for 2022, we have assumed that the growth rate of the cyber sector in 2022 will match the growth rate in 2021. This is, nonetheless, in line with the growth trend for the past few years.
- To calculate the ratio of cyber security employees within the cyber sector to those outside the cyber sector, we have assumed that the core cyber security job vacancies, as defined in Chapter 7 of the findings report, are predominantly to fill roles within the cyber sector. This is done on the broad basis that the cyber sector has the greatest demand for people with these high-level technical cyber skills, over and above other economic sectors. In addition, we have assumed that cyber-enabled job vacancies (as defined in Chapter 7) predominantly represent the people employed in cyber security outside the cyber sector. In practice, organisations outside the cyber sector will also employ people in core cyber roles, to a lesser extent.

Appendix A: 2022 questionnaire

INTERVIEWER INSTRUCTIONS IN CAPS
ROUTING/SCRIPTING/TEXT SUBSTITUTION INSTRUCTIONS (I.E. EVERYTHING THAT WILL NOT APPEAR ON THE INTERVIEWER SCREEN) IN RED CAPS
QUESTION/NEW SCREEN LABELS IN BOLD CAPS
Anything that is CATI-only in green
Anything that is WEB-only in blue

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

Introduction

SHOW IF TELEPHONE RESPONDENT (CATI)
CATIINTRO
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, 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. 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/understanding-the-uk-cyber-security-labour-market
- You can also Google the term "Understanding the UK cyber security labour market" to find the same link yourself.
- SAMPLE S_INTROTX

SHOW IF ONLINE RESPONDENT (WEB)
INTROSCREEN
Thank you for taking part in this confidential Ipsos survey about cyber skills.

IF NON-CYBER SECTOR (SAMPLE S_TYPE=1-2): This survey should be completed by the senior person at your organisation with the most knowledge or responsibility for your cyber security? If you outsource cyber security, this would be the person within your organisation responsible for managing that contract.

IF CYBER SECTOR (SAMPLE S_TYPE=3): This survey should be completed by a senior person in the business who oversees recruitment and training, such as a director or owner.

Participation in the survey is voluntary and you can change your mind at any time. To check the survey is legitimate and to view Ipsos' privacy policy, you can visit LINK TO BE CONFIRMED. You can also Google the term "Understanding the UK cyber security labour market" to find the same link yourself.

Reassurance email

SHOW IF TELEPHONE RESPONDENT (CATI)
REASSURANCE_EMAIL
READ OUT IF TELEPHONE RESPONDENT (CATI) AND WANTS REASSURANCE EMAIL
Just so you know, this email has more information about the survey and gives you a unique link to complete all or part of the survey online, if you prefer this.

STANDARD OPTIONS TO SEND REASSURANCE EMAIL

Consent

ASK IF TELEPHONE RESPONDENT (CATI)
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: LINK TO BE CONFIRMED

SINGLE CODE
Yes
No
CODE 2 CLOSES SURVEY

ASK IF ONLINE RESPONDENT (WEB)
Q1x.ONLINERESP
IF NON-CYBER SECTOR (SAMPLE S_TYPE=1-2): Before we get started, can you confirm you are the senior person with most responsibility for your organisation's own cyber security?

IF CYBER SECTOR (SAMPLE S_TYPE=3): Before we get started, can you confirm you are one of the following:

- a senior director in the business
- a member of the executive team (e.g. a Chief Executive)
- a senior member of the team within your business that offers cyber security products or services.

SINGLE CODE
Yes – a senior person
No

ASK IF CYBER SECTOR BUSINESS (SAMPLE S_TYPE=3)
Q1y.CONSENTC
Your business may have taken part in an Ipsos survey for DCMS in May, June or July 2021, 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 TELEPHONE RESPONDENT AND NOT SKIPPING QUESTIONS (CATI AND CONSENTCDUM NOT CODE 1)
PROFILEINTRO
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 we 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 we 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
WEB: I am the sole trader CLOSE SURVEY IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
CATI: 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 TELEPHONE RESPONDENT AND OUTSOURCE (CATI AND OUTSOURCE CODE 1)
OUTSOURCEINTRO
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

CATI: ASK AS A GRID
WEB: ASK AS A CAROUSEL
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 TELEPHONE RESPONDENT AND NOT CYBER SECTOR (CATI AND TYPXDUM NOT CODE 4)
WORKFORCEINTRO
Now I'd like to ask some questions about you and others **within** your organisation.

SHOW IF ONLINE RESPONDENT AND NOT CYBER SECTOR (WEB AND TYPXDUM NOT CODE 4)
WORKFORCESCREEN
The following questions are 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?
WEB: Please write the number next to each category.
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 TELEPHONE RESPONDENT AND CYBER SECTOR AND MORE THAN ONE PERSON IN A CYBER ROLE (CATI AND CYBERSIZEDUM≠1)
CYBERINTRO
Now we 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.

SHOW IF ONLINE RESPONDENT AND CYBER SECTOR AND MORE THAN ONE PERSON IN A CYBER ROLE (WEB AND CYBERSIZEDUM≠1)
CYBERSCREEN
Now we 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?
WEB: Please write the number next to each category.
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

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
Q18d.JOBROLENUM
IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Do you specialise in any of the following roles?
ADD IF NECESSARY: If you work across multiple roles, this would be the role in which you spend most of your time.
IF MORE THAN ONE (CYBERSIZEDUM≠1): Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, including you, how many specialise in any of the following roles?
ADD IF NECESSARY: If they work across multiple roles, this would be the role in which they spend most of your time.
WEB: Please write the number next to each category.
READ OUT

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP h LAST
a. Security governance, risk, compliance and legal
b. Network security (i.e. networks and firewalls)
c. System security (i.e. operating systems and patching)
d. Penetration testing
e. Security architecture
f. Security operations (e.g. intrusion detection)
g. Incident management, response and recovery
h. A generalist cyber security role

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)
Q18e.JOBROLEPER
Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, including you, roughly what percentage specialise in any of the following roles?
READ OUT
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP h LAST
a. Security governance, risk, compliance and legal
b. Network security (i.e. networks and firewalls)
c. System security (i.e. operating systems and patching)
d. Penetration testing
e. Security architecture
f. Security operations (e.g. intrusion detection)
g. Incident management, response and recovery

h. A generalist cyber security role

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 TELEPHONE RESPODENT AND CYBER SECTOR (CATI AND TYPEXDUM CODE 4)
DIVERSITYINTRO
These next questions help the government to measure diversity across the whole cyber security sector. The answers won't be linked to your business.

SHOW IF ONLINE RESPODENT AND CYBER SECTOR (WEB AND TYPEXDUM CODE 4)
DIVERSITYSCREEN
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
WEB: ASK AS A CAROUSEL

a. IF CYBER SECTOR (TYPEXDUM CODE 4): Complementary 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

CATI: WRITE IN RANGE 0 TO 10
WEB: 0-10 SINGLE CODE SCALE, ALLOW REVERSED SCALE
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
INTERVIEWER NOTE: IF CONFIDENCE LEVELS VARY ACROSS STAFF MEMBERS, THIS IS ABOUT THE MOST CONFIDENT STAFF MEMBER

RANDOMISE STATEMENT ORDER
WEB: ASK AS A CAROUSEL
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
FOR STATEMENTS e AND g ONLY: DO NOT READ OUT: Not applicable – no devices belonging to organisation

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
WEB: ASK AS A CAROUSEL

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
WEB: ASK AS A CAROUSEL

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 TELEPHONE RESPONDENT AND NOT CYBER SECTOR (CATI AND TYPEXDUM NOT CODE 4)
WIDERINTRO
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.

SHOW IF ONLINE RESPONDENT AND NOT CYBER SECTOR (WEB AND TYPEXDUM NOT CODE 4)
WIDERSCREEN
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
WEB: ASK AS A CAROUSEL
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
WEB: ASK AS A CAROUSEL
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
FOR STATEMENT d ONLY: DO NOT READ OUT: Not applicable – no devices belonging to organisation

Training and upskilling

READ OUT IF TELEPHONE RESPONDENT AND NOT CYBER SECTOR (CATI AND TYPEXDUM NOT CODE 4)
TRAININTROA
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 TELEPHONE RESPONDENT AND CYBER SECTOR (CATI AND TYPEXDUM CODE 4)
TRAININTROB
Now I'd like to ask about formal training and upskilling around cyber security.

SHOW IF ONLINE RESPONDENT AND NOT CYBER SECTOR (WEB AND TYPEXDUM NOT CODE 4)
TRAINSCREENA
Now we'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.

SHOW IF ONLINE RESPONDENT AND CYBER SECTOR (WEB AND TYPEXDUM CODE 4)
TRAINSCREENB
Now we'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 TELEPHONE RESPONDENT AND CYBER SECTOR (CATI AND TYPEXDUM CODE 4)
RECRUITINTRO
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 2020, 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 2020, 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
INTERVIEWER NOTE: IF JUST "ANALYST" OR "CONSULTANT", PROMPT WITH SPECIALIST ROLES BEFORE CODING "OTHER".

MULTICODE RESPONSES UNDER THE UNDERLINED HEADINGS UP TO HARD
<u>Generalist roles</u>
Generalist cyber security role
Generalist IT role
Generalist sales role
Senior management role (e.g. CEO or COO)

<u>Specialist roles</u>
Security governance, risk, compliance and legal
Network security (i.e. networks and firewalls)
System security (i.e. operating systems and patching)
Penetration testing
Security architecture
Security operations (e.g. intrusion detection)
Incident management, response and recovery
Threat analyst (i.e. analysing intelligence on cyber threats)
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 2020, 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 TELEPHONE RESPONDENT AND CYBER SECTOR (CATI AND TYPEXDUM CODE 4)
TURNOVERINTRO
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?
WEB: Please write the number next to each category.
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 willing to be invited to a more bespoke interview with Ipsos within the next six months, to further explore the issues of cyber security, skills and recruitment? You don't have to agree to take part now, just indicate your willingness to be asked closer to the time.
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 we please take an email address for this?
IF DON'T WANT REPORT (REPORT CODE 2): Can we 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 IF TELEPHONE RESPONDENT (CATI)
GDPRINTRO
Thank you for taking the time to participate. You can access the privacy policy on our website at: LINK TO BE CONFIRMED. 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.

SHOW IF ONLINE RESPONDENT (WEB)
GDPRSCREEN

Thank you for taking the time to participate. You can access the privacy policy on our website at: LINK TO BE CONFIRMED. 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 card offered to survey respondents

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 is the government's advice campaign on how to stay secure online. It covers six essential actions that organisations and their staff should take to make themselves cyber secure.

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data

You can create your own free Cyber Action Plan in under 5 minutes on the Cyber Aware website.

You can also attend a free online training module "Top tips for staff" which takes less than 30 minutes.

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.

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

Government guidance for organisations on cyber security

Department for Digital, Culture, Media & Sport

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. You can see if you are ready for Cyber Essentials certification, using IASME's readiness tool.

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 46 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. The 10 steps cover:

1. Risk management
2. Staff engagement and training
3. Asset management
4. Security architecture and secure configurations
5. Vulnerability management
6. Identity and access management
7. Data security
8. Logging and monitoring
9. Incident management
10. Supply chain security

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 firms and other larger organisation interviews

Introduction	Timings
▪ Thank participant for taking part. ▪ Introduce self and Ipsos ▪ DCMS wants to understand in more depth current and future cyber skills gaps, and their impact on recruitment to help inform future government policy ▪ All responses are confidential and anonymous ▪ **Incentive:** £50 ▪ **Recording:** get permission to digitally record. ▪ **Length:** Approx. 50-60 mins **GDPR added consent (once the recorder is on)** Ipsos' 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?	2-3 minutes
Context and main challenges	**Timings**
Interviewers will do some background reading about the organisation before the interview, and the participant's role in recruitment and training will be collected in the screening process. ▪ Can you briefly summarise your background and knowledge of cyber security before taking on this role? ▪ Right now, what are the main challenges and gaps when it comes to cyber skills in your organisation? What would you say are the top 2-3 issues? ▪ Are there particular cyber skills functions that are proving a challenge? What do these mean for your organisation?	5 minutes
Training and qualifications	**Timings**
Summarise main challenges/regional challenges ▪ What have your main challenges been in terms of training people in cyber roles? ▪ What have your main challenges been in terms of training or raising awareness among wider staff on cyber security? ▪ What are the gaps in your cyber security training? What improvements would you like to see? What changes are you planning or considering? ▪ What impact has remote or hybrid working had on cyber security training? **External training** IF USE EXTERNALLY DEVELOPED/DELIVERED TRAINING (FROM SURVEY): ▪ How do you select external providers? What are the most important criteria? ▪ How easy is it to find the right external training? Where do you look? What does good external training look like? PROBE: any geographic challenges finding training in this region/local area?	15-20 minutes

▪ How do you judge whether the provision is value for money? How do you evaluate its effectiveness? **Qualifications** ▪ How important is it for staff in any cyber roles in your organisation to have specific qualifications? ▪ What types of qualifications are most valuable? IF NO QUALIFIED STAFF (FROM SURVEY): ▪ You mentioned when we interviewed you, that none of your staff in cyber roles have or are working towards qualifications in cyber security. Can you explain this a bit more? ▪ How do you validate the skills of these staff without qualifications? What are the alternatives? ▪ Have they had relevant training that does not lead to qualifications? What was behind this decision? **Career pathways and Continuing Professional Development (CPD)** ▪ What thinking/work have you done around career pathways/progression for those in cyber roles in your organisation? ▪ Have you developed career pathways internally? What did you use to inform these career pathways? Have you used any external resources? ▪ What have the challenges been in creating career pathways? What lessons have you learnt? PROBE: more difficult for particular roles? ▪ How does your organisation approach the Continuing Professional Development (CPD) of people in cyber roles? How do you keep their skills up to date? ▪ How important is this kind of CPD to the senior management in your department? In the organisation as a whole? **The UK Cyber Security Council** *Participants will have been sent a link to the UK Cyber Security Council Careers Route Map before the interview. If they have not taken a look, give them a minute to look at this link and click through some of the categories: https://www.ukcybersecuritycouncil.org.uk/careers-learning/careers-route-map/* ▪ Had you heard of the UK Cyber Security Council before we got in touch with you? What had you seen/heard? ▪ Would this map be helpful for your cyber team/business? Is there anything that could be added/ improved that would make it more helpful? **Cyber Security Body Of Knowledge (CyBOK)** *Participants will have been sent a link to the CyBOK website and manual before the interview. If they have not taken a look, read out this description from DCMS:* CyBOK is a body of knowledge to inform and underpin education and professional training for the cyber security sector. It covers 21 distinct knowledge areas and is maintained by the cyber security community. ▪ What had you seen or heard about the CyBOK knowledge framework before this interview? Had you used anything like this before the interview? ▪ Would this framework be helpful for your cyber team/business?	
Cyber recruitment	**Timings**
Summarise main challenges/regional challenges IF RECRUITED (FROM SURVEY AND SCREENER): ▪ What have your main challenges been when recruiting people for cyber roles?	15-20 minutes

▪ What kinds of recruitment are most challenging? E.g. different job roles, specialisms, seniority levels? ▪ PROBE: any specific challenges with: penetration testing, cyber security architecture, cyber risk management, incident response and management? ▪ PROBE: any geographic challenges recruiting in this region/local area? What's your perception of the talent pool in this region? How well does it fit your needs? What steps have you taken to overcome any challenges? ▪ What impact has remote or hybrid working had on recruitment into cyber roles in your organisation? PROBE: changing how they recruit geographically, changing demands from candidates? IF HARD-TO-FILL VACANCIES (FROM SURVEY) ▪ You mentioned in the survey that you recently had vacancies for cyber roles that you found hard to fill. Can you tell me about your experience? PROBE: nature of role, how advertised, how long it was open ▪ Did you change your recruitment approach? What steps did you take? What impact did any changes have? PROBE: changing recruitment channels, altering job requirements/descriptions, changing pay/benefits ▪ Have these vacancies now been filled? What made the difference? What lessons have you learned? **Assessing competency and perceived quality of recruits** ▪ How do you assess whether job applicants are proficient? What do you especially look for? What raises concerns/stands out? PROBE: qualifications, training, background and experience, tests, CVs, complementary skills (communication, teamworking etc.) ▪ What has the quality of staff recruited in the last 2 years been like compared to your original expectations and needs? How have they exceeded/not met expectations? ▪ What do you think of the idea of a Chartered Cyber Security Professional status? How helpful would this be to your organisation in training/recruitment? **Salaries** ▪ How do you determine salaries for staff in cyber roles? ▪ Do you know the market rate? What work have you done to research this? ▪ Do you pay higher salaries to staff in cyber roles vs. other technical roles (e.g. in IT roles)? What's behind this decision? ▪ Do certain cyber roles get offered higher salaries? Do people with specific cyber skills/qualifications/training get offered higher salaries? **Entry level roles/apprenticeships** ▪ Do you offer/intend to offer entry-level roles/apprenticeships or other work placements in cyber security for new joiners? What's behind your decision? ▪ What are the challenges of introducing these kinds of entry-level roles (PROBE APPRENTICESHIPS SPECIFICALLY)? How have you/might you address these? What support would be helpful?	
Diversity in cyber teams	**Timings**
Understanding of diversity ▪ What do you think I mean when I talk about diversity in the cyber sector/in cyber teams? What kinds of characteristics do you think this refers to? Which ones are most important? ▪ How big an issue is this for the cyber sector, in your opinion? What kinds of diversity do you think are lacking? ▪ How important a consideration is diversity in your cyber teams? How has this changed/evolved in the last 2 years? What specific changes have you seen?	15 minutes

▪ Have there been any changes in *your own organisation's* approach to diversity in the last 2 years? Have these changes been specific to the cyber part of the organisation, or across the wider organisation **Their impact on diversity** ▪ How diverse are the people applying to you for cyber jobs? Why do you think this is? ▪ What control do you have over the diversity of your applicants? How diverse are your recruitment channels? PROBE: use of networks to recruit and impact this might have **Role of HR colleagues** ▪ How are HR colleagues involved in the recruitment process for cyber roles? What is the extent of their involvement? ▪ How much do you consult/hear from HR colleagues on diversity in cyber teams/cyber recruitment? **Changes made in recruitment process** IF TAKEN ACTION ON DIVERSITY (FROM SURVEY) ▪ You mentioned in the survey that you have taken action to improve diversity in your recruitment. Tell me about this experience. ▪ What prompted you to do this? ▪ What has the impact been? What has worked well? What lessons did you learn?	
Wrap-up	**Timings**
▪ Across all the challenges we have discussed, what do you think the government should be doing to address these things? ▪ What should industry be doing? ▪ What should your organisation's senior management be doing/focused on? THANK PARTICIPANT AND CLOSE INTERVIEW. REMIND THEM OF CONFIDENTIALITY AND £50 INCENTIVE. CHECK IF THEY HAVE PROVIDED DETAILS TO MAKE THE INCENTIVE PAYMENT.	2-3 minutes

Appendix C: Topic guide for recruitment agent interviews

Introduction	Timings
▪ Thank participant for taking part. ▪ Introduce self and Ipsos ▪ DCMS wants to understand in more depth current and future cyber skills gaps, and their impact on recruitment to help inform future government policy ▪ All responses are confidential and anonymous ▪ **Incentive:** £100 ▪ **Recording:** get permission to digitally record. ▪ **Length:** Approx. 50-60 mins **GDPR added consent (once the recorder is on)** Ipsos' 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?	2-3 minutes
Context	**Timings**
Interviewers will do some background reading about the organisation before the interview, and the participant's role in recruitment and training will be collected in the screening process. ▪ Can you briefly summarise your background and any technical knowledge of cyber security? ▪ Right now, what are the main challenges when it comes to the kinds of cyber roles you help recruit? What would you say are the top 2-3 issues? ▪ Are there particular cyber skills functions that are proving a challenge for recruiters to fill? Can you summarise what makes these so difficult? INTERVIEWER: JUST ASK FOR A QUICK RESPONSE AND SAY WE WILL COME BACK TO THESE THINGS LATER IN THE INTERVIEW	5 minutes
Current recruitment pool	**Timings**
How the recruitment pool has changed ▪ Approximately, how many active and passive cyber candidates do you have on your books (SEE NOTES)? How has this changed compared to 2019 and 2020? ▪ How does this vary by region? Are there any certain regions that have a larger pool? What is driving this? How has this changed compared to 2019/2020? ▪ How has COVID-19 changed the recruitment pool? What changes have persisted/will persist in 2021/under remote/blended working? ▪ How does the profile/quality/calibre of candidates in the cyber recruitment pool compare to 2019/2020? PROBE: typical experience/seniority, sector backgrounds, education/qualifications ▪ Roughly what proportion come from a cyber background already vs. those looking to transition into cyber roles? What sectors do those looking to transition come from? How does this compare to 2019/2020? **Gaps in the recruitment pool**	15 minutes NOTES: Active = actively looking for a job/move Passive = not actively looking

▪ What would you say the biggest gaps in the recruitment pool are at the moment? INTERVIEWER: IF ALREADY RAISED EARLIER IN CONTEXT SECTION, THEN PROBE IN MORE DETAIL NOW ▪ PROBE: any specific challenges with: penetration testing, cyber security architecture, cyber risk management, incident response and management? ▪ How does this compare to 2019/2020? ▪ What do you think is behind these gaps? ▪ How realistic is it to source these sorts of candidates/fill these gaps in the pool? How have you gone about filling these sorts of gaps? **Sourcing candidates** ▪ How do you go about sourcing cyber candidates? What are the most and least effective methods for finding good quality candidates? ▪ How do you assess whether job candidates are proficient? ▪ What do you especially look/stands out for when you put candidates on your books? And when you send them to an employer? PROBE: qualifications, training, background and experience, tests, CVs, complementary skills (communication, teamworking etc.) ▪ Have these methods changed since 2019/2020? How have you refined/evolved your approach? What lessons have you learnt over the past year? ▪ Does the approach differ by region? Are there particular regions that are harder to source candidates from? What is causing this? What's the impact of these regional differences?	
Diversity	**Timings**
Diversity of candidate pool Next, we would like to talk about the diversity of the current candidate pool. This includes things like socioeconomic status, gender balance, ethnicity, having a physical disability, or any neurodiverse condition or learning disorder. ▪ How would you describe the diversity of the current candidate pool? PROBE: in terms of socioeconomic status, gender, ethnicity, disability and neurodiversity ▪ How does this compare to 2019/2020? In what ways has the recruitment pool improved/got worse? ▪ What kind of monitoring/information do you have on the diversity of the candidates on your books? **Support needs of diverse candidates** ▪ What kinds of support do people from these sorts of diverse backgrounds need to succeed in the cyber security labour market? ▪ What reasons might candidates from diverse groups be unsuccessful? ▪ What do you do to encourage these sorts of candidates to apply? What kind of support do you offer in this area? What has been successful? ▪ How well do employers support the needs of these candidates currently? What are the most important improvements they could make to encourage these sorts of candidates to enter cyber roles? ▪ Do they tend to come from/prefer certain education/training/career pathways into these roles? **Cyber employer attitudes to diversity** ▪ What demands do clients hiring for cyber roles typically make of you when it comes to diversity? ▪ Are there any diversity quotas clients ask for on the shortlisted candidates? Is it HR or the cyber hiring manager who typically ask for this?	10 minutes

▪ How often do clients ask for your advice/guidance when it comes to diversity? What do you see as your role in this area? Do you feel that recruiters have any responsibilities in this area? ▪ Have your clients' attitudes towards diversity changed since 2019/2020? How has this affected what they demand from you? ▪ Are there any regional differences in attitudes? ▪ In our previous study, we found that hiring managers for cyber roles often lacked awareness of workforce diversity issues. Would you say this is still the case?	
Recruitment criteria	**Timings**
<u>Summarising client demands</u> ▪ What are your clients' biggest needs presently, when recruiting for cyber roles? PROBE: specific skills, roles, qualifications, experience levels ▪ How have these needs evolved since 2019/2020? What requirements have become more acute this year? ▪ Do clients have typical minimum requirements? INTERVIEWER: IF QUALIFICATIONS OR EXPERIENCE REQUIREMENTS RAISED HERE, THEN USE DISCUSSION PROMPTS IN THE NEXT TWO SUBSECTIONS ▪ How realistic is it to meet these demands from the current cyber candidate pool? **<u>Regional differences</u>** ▪ How does this vary according to location? Do clients in certain regions have different skills requirements? How has this changed over the past year? ▪ How important is the location of candidates to clients? How has this changed over the past year? PROBE: are they willing to accept candidates from further afield in the UK than before? International candidates? ▪ What changes have persisted/will persist in 2021/under remote/blended working? **<u>Qualifications</u>** ▪ What kind of formal qualifications are clients typically looking for? What makes a candidate stand out? PROBE: higher education vs. other technical qualifications ▪ Has the demand for certain qualifications changed since 2019/2020? ▪ How easy is it to fulfil these qualification requirements from the existing candidate pool? How does this compare to past years? ▪ How flexible are clients in these demands? Are they willing to accept alternative candidates that don't meet their initial demands in terms of qualifications? **<u>Experience</u>** ▪ Typically, how many years of experience do your clients look for? ▪ What kind of experience do employers value? PROBE: industry vs. other roles, candidates transitioning from non-cyber roles (what do they need)? ▪ Has the demand for certain experience changed since 2019/2020? ▪ How easy is it to fulfil these experience requirements from the existing candidate pool? How does this compare to past years? ▪ How flexible are clients in these demands? Are they willing to accept alternative candidates that don't meet their initial demands in terms of experience? **<u>Unrealistic job adverts</u>** ▪ What involvement do you typically have in drafting clients' job descriptions/ adverts? ▪ In your view, how well-written are the job descriptions/adverts that come to you? Do clients have realistic expectations? What aspects tend to be challenging to fulfil? Has this changed since 2019/2020?	15 minutes

▪ How certain are clients of what they want/need when recruiting for cyber roles? ▪ If a client provides unrealistic job descriptions/adverts, how do you approach this? What steps do you take? How flexible are they to amendments?	
Keeping up to date and engagement	**Timings**
<u>Relationships with hiring managers and HR</u> ▪ How would you describe your relationships with hiring managers? What level of engagement/discussion do you get from them? How willing are they to listen to your advice/guidance? ▪ When recruiting for cyber roles, how involved are HR staff in your interactions with clients? What aspects do they get involved in? PROBE: diversity, job descriptions **<u>Keeping up to date</u>** ▪ How much feedback do you get from your clients on candidates you have sent? PROBE: feedback during recruitment, e.g. after interviews, and later, after candidates are in post ▪ How useful is the feedback you receive? ▪ How do you keep up to speed with developments in cyber skills, training and employers' needs generally? PROBE: talking to employers, other recruiters, conferences, magazines/websites, networks ▪ How easy is it to stay up to date? ▪ How much would you say you know about the latest cyber security training and qualifications? **<u>The UK Cyber Security Council</u>** *Participants will have been sent a link to the UK Cyber Security Council Careers Route Map before the interview. If they have not taken a look, give them a minute to look at this link and click through some of the categories: https://www.ukcybersecuritycouncil.org.uk/careers-learning/careers-route-map/* ▪ Had you heard of the UK Cyber Security Council before we got in touch with you? What had you seen/heard? ▪ Had you used anything like this map before the interview? Have your clients used/referred to this? ▪ Would this map be helpful for recruiters? Is there anything that could be added/ improved that would make it more helpful? ▪ What do you think of the idea of a Chartered Cyber Security Professional status? How helpful would this be to your organisation in training/recruitment? **<u>Cyber Security Body Of Knowledge (CyBOK)</u>** *Participants will have been sent a link to the CyBOK website and manual before the interview. If they have not taken a look, read out this description from DCMS:* CyBOK is a body of knowledge to inform and underpin education and professional training for the cyber security sector. It covers 21 distinct knowledge areas and is maintained by the cyber security community. ▪ What had you seen or heard about the CyBOK knowledge framework before this interview? ▪ Do your clients use/refer to this framework? ▪ Would this framework be helpful for recruiters?	10 minutes

Wrap-up	Timings
▪ Across all the challenges we have discussed, what do you think the government should be doing to address these things? ▪ What should industry be doing? ▪ What should your organisation's senior management be doing/focused on? THANK PARTICIPANT AND CLOSE INTERVIEW. REMIND THEM OF CONFIDENTIALITY AND £100 INCENTIVE. CHECK IF THEY HAVE PROVIDED DETAILS TO MAKE THE INCENTIVE PAYMENT.	2-3 minutes

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

ISO 20252

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

Market Research Society (MRS) Company Partnership

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

ISO 9001

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

ISO 27001

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

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

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

HMG Cyber Essentials

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

Fair Data

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

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

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

About Ipsos Public Affairs

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