Cyber security skills in the UK labour market and cyber security sectoral analysis 2025

Technical report

Jayesh Shah, Jamie Douglas, Alex Bollen, Sophia Hasapopoulos, Shahil Parmar, Grace Clarke, Ipsos
Sam Donaldson, Perspective Economics

Department for Science, Innovation & Technology

Ipsos

23-089495-01 Ipsos | Cyber security skills in the UK labour market and cyber security sectoral analysis 2025: technical report | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252.

Contents

1 Overview

1.1 Introduction

The Department for Science, Innovation and Technology (DSIT) commissioned Ipsos and Perspective Economics to conduct the latest in an annual series of studies to improve its understanding of the current UK cyber security sector. This year, for the first time, the Cyber Security Skills in the UK Labour Market Study (henceforth, Cyber Security Skills Study) and the UK Cyber Security Sectoral Analysis were combined into a single survey.[1]

In February 2023, Machinery of Government changes moved responsibility for cyber security from the Department for Culture, Media and Sport (DCMS) to DSIT. DSIT have been responsible for publishing the last 2 releases of both the Cyber Security Skills Study and UK Cyber Security Sectoral Analysis.

In this technical report and the associated publication, we refer to a report by its year of publication, rather than the year in which fieldwork was conducted. For example, the 2024 report for Cyber Security Skills Study covers findings from fieldwork conducted in 2023. Links to previous reports and the year in which fieldwork was conducted for each report can be found in Table 1.1 and Table 1.2.

Table 1.1: Previous publications for Cyber Security Skills Study

Year of report publication	Year when fieldwork was conducted	Published by
2024 report	2023	DSIT
2023 report	2022	DSIT
2022 report	2021	DCMS
2021 report	2020	DCMS
2020 report	2019	DCMS
2018 report	2018	DCMS

Table 1.2: Previous publications for Cyber Security Sectoral Analysis

Report	Year when fieldwork was conducted	Published by
2024 report	2023	DSIT
2023 report	2022	DSIT
2022 report	2021	DCMS
2021 report	2020	DCMS
2020 report	2019	DCMS
2019 report	2018	DCMS

This report provides the technical details for all strands of the 2025 report, and copies of the main survey instruments (in the appendices) to help interpret the findings. DSIT has published separate reports of the main findings from the research for the Cyber Security Skills Study and Cyber Security Sectoral Analysis.

1.2 Full research objectives

This 2025 report (which covers research conducted in 2024), in line with previous years, aimed to gather evidence on:

[1] Ipsos and Perspective Economics would like to thank colleagues at DSIT for their project management, support and guidance throughout the study.

Cyber Security Skills Study:

- Current cyber security skills gaps
- Current skills shortages and impacted job roles
- Outsourcing to fill cyber security skills gaps
- Diversity within the cyber security sector
- Staff turnover in the cyber security sector
- Size of the UK's cyber security recruitment pool
- Overall cyber security workforce gap
- Role of recruitment agents and training providers in the cyber security labour market

Cyber Security Sectoral Analysis:

- Profile of UK cyber security businesses
- Location of UK cyber security businesses
- Economic contribution of the UK cyber security sector
- Investments in the UK cyber security sector
- Supporting growth of the UK cyber security sector

1.3 Summary of methodology

The methodology for both the Cyber Security Skills Study and Cyber Security Sectoral Analysis consisted of 4 strands:

1. **Quantitative surveys** – Ipsos conducted representative telephone surveys with 4 audiences: general businesses, public sector organisations, charities and cyber security sector businesses. In line with previous years, questions included in the Cyber Security Sectoral Analysis report were only asked to those in the cyber security sector. Pilot fieldwork was conducted between 31st July and 5th August 2024 and mainstage fieldwork was between 7th August and 18th October 2024. There was also a short recall survey, which took place between 18th November and 29th November 2024, to fill in missing responses to the survey question Q30_Managerial due to a technical issue.

2. **Qualitative interviews** – Ipsos conducted a more focused strand of qualitative research, completing 50 in-depth interviews. The breakdown of this number by audience type is as follows: 24 in-depth interviews with cyber security businesses, 11 in-depth interviews with cyber security leads in large and medium businesses or public sector organisations, 5 in-depth interviews with investors, 4 in-depth interviews with recruitment agents and 6 in-depth interviews with cyber security training providers. The interviews explored the challenges organisations faced in addressing skills gaps and shortages, approaches to recruitment, workplace diversity, and factors impacting investment and support for the development of skills in the cyber security workforce. Interviews took place between 16th September and 26th November 2024.

3. **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Lightcast labour market database, providing details on the number, type and location of job vacancies across the UK. This database also covers remuneration, descriptions of job roles and the skills, qualifications and experience being sought by employers. This work primarily covered vacancies across the calendar year in 2024 (12 months), supplementing the work done in the 2024 study (which covered vacancies from January 2023 to December 2023).

4. **Supply side analysis** – Perspective Economics replicated the methodology used in the 2024 study 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 2024). This strand produces further statistics on the demographic diversity, educational and occupational backgrounds, and salaries of this pool of labour, as well as outflows from the pool.

1.4 Similarities and differences from the 2024 report studies

The quantitative surveys for the Cyber Security Skills Study and Cyber Security Sectoral Analysis projects were merged together, necessitating the removal of a number of questions that were asked in previous years.

The 2025 report methodology for secondary data analysis is consistent with previous years. This means that we can look at trends over time across the job vacancies analysis and supply side analysis.

Questionnaire changes

The quantitative survey questions were reviewed and revised to ensure we capture the metrics that are most useful for DSIT and its stakeholders, while keeping the length of the survey manageable

to participants. This year as well as removing questions, we included new questions around whether organisations outsource cyber security outside the UK and AI usage among cyber security businesses. As such, we are not able to look at trends over time for these new questions. The rationale for the questionnaire changes is provided in Section 2.1.

Although the Cyber Security Skills Study and Cyber Security Sectoral Analysis surveys have been merged and new questions have been added, question wording and phrasing have remained consistent with previous years where possible, so have not undergone cognitive testing. However, a live pilot of the quantitative survey was run prior to the full survey to ensure questions were understood correctly (see Section 2.3).

Sample sizes

The sample size achieved for the cyber security businesses in the quantitative survey is in line with the previous year for the Cyber Security Sectoral Analysis and an increase from the Cyber Security Skills Study. There was also a higher response across businesses in the private sector and charities, whereas there was a slightly lower public sector response compared to the 2023 Cyber Security Skills Study.

This year we interviewed:

- 209 cyber security businesses
- 1,061 businesses across the private sector, of which 48 were large businesses
- 111 public sector organisations
- 197 charities

Table 1.3 and Table 1.4 provide the number of surveys achieved for these audiences in previous waves of the Cyber Security Skills Study and Cyber Security Sectoral Analysis, respectively.

Table 1.3: Number of surveys achieved for previous waves of the Cyber Security Skills Study

Report	Cyber security businesses	Businesses across the private sector	Public sector organisations	Charities
2025 report	209	1,061 (of which 48 were large)	111	197
2024 report	180	930	130	190
2023 report	180	1,006 (of which 78 were large)	102	214
2022 report	224	947 (of which 107 were large)	123	211
2021 report	171	965 (of which 65 were large)	76	220

Table 1.4: Number of surveys achieved for previous waves of the Cyber Security Sectoral Analysis

Report	Cyber security businesses
2025 report	209
2024 report	210
2023 report	220
2022 report	248
2021 report	262

The margin of error for the overall business sample is similar to last year, at ±2-3 percentage points (from ±2-4 percentage points in 2024). The margin of error has remained broadly consistent for large businesses at ±9-14 percentage points in this 2025 report (matching the ±9-14 percentage points in the 2024 report). In this 2025 report, the margin of error across other organisations has also remained consistent, for public sector organisations it was ±6-9 percentage points in (comparable to the ±5-9 percentage points in the 2024 report) and ±4-7 percentage points for both charities and cyber security businesses (matching the ±4-7 percentage points for both in the 2024r eport). Margins of error assume 95% confidence level.

1.5 Differences from other recent studies looking at cyber security skills

A note on the UK cyber security workforce size estimate from the 2023 Cyber Security Workforce Study

The International Information System Security Certification Consortium (ISC2) is a global membership organisation for cyber security professionals. It publishes an annual Cyber Security Workforce Study, the most recent of which was published in 2024. This is a study of the global cyber security workforce and largely reports its findings at a global level.

The 2024 ISC2 report suggests there are c.349,360 individuals in the UK cyber security workforce, with a shortage of c.93,349. This differs greatly to our estimate, but the estimates are not comparable due to the vast differences in methodologies between our studies (outlined later in this section) and a lack of published technical information on the UK sample size and representativeness of the ISC2 data. Their estimate is also likely to have a substantive margin of error around it.

The ISC2 estimate has fluctuated across years, from c.365,823 in 2020, 300,087 in 2021, 339,145 in 2022, 367,300 in 2023, and 349,360 in 2024. In our opinion, it remains unrealistically high. This would mean that almost 1 in every 100 employees in the UK are working in a cyber security role. Furthermore, the DSIT Sectors Economic Estimates indicate that there were c.1.84 million jobs across all UK digital sectors between April 2023 to March 2024. If the ISC2 estimate was correct, this would mean that around 1 in 5 digital sector jobs are in cyber security.

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

The findings from the ISC2 2024 report touch on similar themes to the Cyber Security Skills Study (such as skills gaps, diversity in the cyber security sector and qualifications) but they are not directly comparable. This is also the case for other well-known surveys that have been published over recent years, the NCSC/KPMG Decrypting Diversity 2021 report, the PwC Cyber Security Strategy 2022 and PwC Cyber Security Outlook 2023 report.

Our study offers several advantages:

- 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.
- 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 majority of all businesses and charities in the UK.
- Our cyber security 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 security businesses.

- 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 6 of the main report for full details). This continues the methodology from the 2 previous studies.

2 Quantitative survey

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

2.1 Questionnaire development

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).

In line with the surveys for the Cyber Security Skills Study 2024 and Cyber Security Sectoral Analysis 2024 reports, the questionnaire worked as a multimode telephone and online survey script – this is covered further in Section 2.4. Changes reflect new areas that DSIT wished to study, as well as questions that needed to be removed to reduce survey length. Appendix A includes a copy of the final questionnaire used in the main survey.

Questions that were added this year were around outsourcing outside of the UK, awareness of the UK Cyber Security Council, future recruitment activity levels and AI. **Questions that were added this year were:**

- Q14a_WHATOUTNONUK: Do you outsource any of the following to individuals or organisations outside the UK?
- Q14b_WHATHIGHERNONUK: Which of the following specific higher-level functions do you outsource outside the UK? – It is worth noting that this question was not able to be reported in the findings report as the base size was very low under 30.
- Q18x_COUNCILAWARE: The UK Cyber Security Council is the self-regulatory body for the UK's cyber security profession. Before this interview, had you heard of the UK Cyber Security Council?
- Q47e_DIVERSEACTION: Since the start of 2023, have you carried out any of the following to encourage applications from diverse groups?
- Q47f_FUTURE: Over the next 12 months, compared with the last 12 months, do you expect your recruitment activity to increase, stay about the same, or decrease?
- Q47g_AIUSE: Currently, does anyone in a cyber security role in your business use AI skills as part of their day-to-day work?
- Q47h_AIRECRUIT: Since the start of 2023, have you recruited anyone with AI skills into a cyber security role?
- Q47i_AITRAIN: Since the start of 2023, has anyone in a cyber security role in your business, including you, received training on AI concepts or algorithms?
- Q47j_AIFUTURE: Over the next 12 months, compared with the last 12 months, do you expect the need for AI skills among people in cyber security roles in your business to increase, stay the same or decrease?

Questions that were in the previous year's Cyber Security Skills Study that were removed were:

- Q18_PATHWAY: Of all the people directly involved in cyber security within your organisation, how many entered this role in each of the following ways?

- Q18f_WEBSITE: For this next question, we would briefly like you to look at a website, which lists the UK Cyber Security Council's 16 cyber security specialisms.[2]
- Q18j_GENERALIST: Which, if any, of the following responsibilities do you consider to be part of your employees Cyber Security Generalist role?
- 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?
- Q23_WHICHQUALS: Which of the following types of qualifications or certified training do you or other employees have, or are they working towards?
- Q26_FORMAL: Is cyber security a formal part of your job description, or do you cover this role informally?
- Q47e_REASON: As far as you know, what reasons did employees have for leaving of their own volition?
- Q43_RECRUIT: Since the start of 2022, have you tried to recruit anyone to fill any cyber security skills needs in your organisation? This includes any current vacancies you may have.
- Q44_OTHRECRUIT: What recruitment methods have you used to find candidates for these vacancies?
- Q47_HARDREASON: What are the reasons these vacancies have been hard to fill?
- 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?
- Q47AB_BARRIERSASK: In the last 18 months, have you carried out any of the following to encourage applications from women, people from ethnic minority backgrounds, disabled people of people with neurodiverse conditions or learning disorders?
- Q47b_INTERN: Since the start of 2022, have you offered any internships or work placements in cyber security roles?
- Q47c_ENTRY: What are the minimum requirements for an entry-level cyber security role in your organisation?
- Q49a_WEBFOLLOW: Finally, can we email you a link to the last question that you weren't able to answer over the phone?
    - This is the question asked about the UK Cyber Security Council's 16 cyber security specialisms.

Questions that were in the previous year's Cyber Security Sectoral Analysis that were <u>removed</u> were:

- Q17_TEAM: Within your organisation, how many people, including yourself, are directly involved in managing or running your organisation's cyber security?
- Q9_PRODSER: Would you describe your business as predominantly offering cyber security-related products, cyber security-related services, or both of these?
- Q1_CONSENT: Before we start, I just want to clarify that participation in the survey is voluntary and you can change your mind at any time. Are you happy to proceed with the interview?[3]
- Q1x_ONLINERESP: 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.

[2] Note that this has since been changed to 15 specialisms following the removal of Cyber Security Generalist.
[3] The consent question from the previous year's Cyber Security Skills Study was retained and became the consent question for the combined survey.

- Q2_NONCYBER: Do you carry out any core business activities, or offer products or services, that are not related to cyber security?
- Q3_SIZE: Across your business in the UK as a whole, how many employees do you have? By that we mean both full-time and part-time employees on your payroll, as well as any directors, working proprietors or owners.
- Q4_SIZEB: Are there approximately … ?
- Q5_CYBERSIZE: How many of your 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.
- Q6_CYBERSIZEB: Are there approximately … ?
- Q29a_SKILLSRECON: Ipsos is carrying out another survey on behalf of DSIT in August and September 2023, which is about the skills, training and recruitment needs of the UK cyber security sector. This is an annual survey that informs DSIT's skills programmes, as well as the work of industry bodies, such as the UK Cyber Security Council. We may randomly sample your business to take part again in that survey. With this in mind, would you be happy for us to securely hold your individual contact details until the end of September 2023, solely for this purpose? You don't have to agree to take part at this stage, just to being invited to take part.
- Q_TEL: Can we just confirm the best telephone number and email address to contact you on?
- Q_SKILLSALTCONTACT: In case we cannot get through to you in August or September 2023, is there anyone else in your business that we could invite to take part on your behalf?
- Q_CHARITYDONATION: As promised, we will make a £10 charity donation on your behalf as a thank you for taking part. We have three charities for you to choose from. Please select one of the following.
- Q43_RECRUIT: Since the start of 2022, have you tried to recruit anyone to fill any cyber security skills needs in your organisation? This includes any current vacancies you may have.

Questions that were in the previous year's Cyber Security Skills Study that had <u>minor alterations</u> made to them but which are still comparable to previous years were:

- For Q13_WHATOUT: Which of the following aspects of cyber security are covered by your outsourced provider or providers?
  - There were minor refinements made to statements i and k:
  - i) Any higher-level functions, which could include things like:
    - security engineering or architecture
    - penetration testing or vulnerability scanning
    - using threat intelligence tools
    - forensic analysis
    - interpreting malicious code
    - autonomous cyber defences
    - or using tools to monitor user activity
  - k) Setting up new user accounts and authentications securely
- For Q14_WHATHIGHER: Which of the following specific higher-level functions are covered by your outsourced provider or providers?
  - There were minor refinements made to statement h:
  - h) Any autonomous cyber defences
- Q29_HIGHTECHNICAL: And how confident, if at all, would you feel about you or any of the other individuals directly involved in cyber security being able to do each of the following high-level technical tasks in your work?

  - There were minor refinements made to statement i:
  - i) Deploying autonomous cyber defences
- Q47_LEFT: In the last 18 months, have any employees in cyber security roles left your company or retired?
  - Minor refinement made to wording "In the last 18 months" was changed to "Since the start of 2023" to be more consistent with the rest of the questionnaire.
- 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?
  - Minor refinements made to wording "In the last 18 months" was changed to "Since the start of 2023" to be more consistent with the rest of the questionnaire – there should be no impact on comparability.
- Q45_VACANCIES: Since the start of 202X, how many vacancies have you had in cyber security roles?
  - This year we allowed people to say 0, as the filter question Q43_RECRUIT was removed. Generally, in our report we do not compare this question across previous years, but if it is, we will have rebased any means/medians to exclude the 0 values.
- Q29_TECHNICAL: How confident, if at all, would you feel about 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?
  - There were minor refinements made to statement p:
  - p) Setting up new user accounts and authentications securely
- Q29_HIGHTECHNICAL: And how confident, if at all, would you feel about you or any of the other individuals directly involved in cyber security being able to do each of the following high-level technical tasks in your work?
  - There were minor refinements made to statement i:
  - i) Deploying autonomous cyber defences
- Q34_CORE: How confident, if at all, would you feel in your organisation’s core staff as a whole being able to do each of the following?
  - The answer statement "Use acceptably strong passwords" was removed this year.

Questions that were in the previous year's Cyber Security Sectoral Analysis but which are still comparable to previous years that had <u>minor alterations</u> made to them were:

- Q20_BARRIERS: To what extent, if at all, have any of the following issues affected your ability to meet your business goals across the last 12 months?
  - Minor refinements were made in wording of statement g:
  - g) Salary demands of candidates not being affordable
- Q15_REGION: In which of the following regions of the world are your non-UK customers based?
  - Minor refinements in question wording.

Questions that were in the previous year's Cyber Security Skills Study that had <u>significant alterations</u> made to them were:

- Q18g_JOBROLE: Do any of the employees working in cyber security roles, including you, specialise in any of these roles?
  - We removed the generalist code and capped answers relative to the number of people in cyber security roles.
- Q46b_HARDROLE: What specific roles or occupations were these hard-to-fill vacancies in?
  - Significant changes were made to answer statements in line with the changes to Q18g_JOBROLE.
- 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?
  - This year this question was not asked to cyber security businesses, it was asked to private sector businesses, public sector organisations and charities. There were also changes made to the answer statements, we removed "Complementary skills, such as oral or written communication skills and team working skills"; "Understanding the legal or compliance issues affecting cyber security, such as data protection" and "Incident response skills".
- Q30_MANAGERIAL: How confident, if at all, would you feel about 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?
  - This year this question was not asked to cyber security businesses, it was asked to private sector businesses, public sector organisations and charities. There were also changes made to the answer statements, j and k are new statements added this year:
  - j) Developing a cyber security strategy, i.e. a document that underpins all your policies and processes
  - k) Assessing whether your external cyber security providers are offering value for money
- Q48b_PANEL: Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, and we are going to contact the UK cyber security sector again in around 12 months. Would you be happy for Ipsos to maintain your individual contact details for 12 months, to save us from having to contact any switchboard next time? Participation in any later years would still be voluntary and you can opt out at any point.
  - This question was previously called DCMSRECON, wording changes were made to this question and this year it was only asked to cyber security businesses whereas previously it had also been asked to private sector businesses.

Questions that were in the previous year's Cyber Security Sectoral Analysis that had <u>significant alterations</u> made to them were:

- Q21b_SPECIALISMS: You said you have had issues with cyber security skills, either among job candidates, or among your existing employees.
  - Significant changes were made as we removed the generalist code.
- Q14_EXPORTB: In your most recently completed financial year, approximately what percentage of your turnover from your cyber security business was attributable to exports? By exports, we mean where products or services are purchased and used overseas by non-UK customers or clients. Was it …?
  - This year we added a "have not started trading yet" code, as we no longer filter out those who are pre-turnover (as we deleted the turnover question). To maintain comparability with previous years, this code, i.e. those who have not started trading yet, should be excluded from the base in analysis.

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 1 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), Central Government Departments were excluded because DSIT expected that Government Departments would not be able to talk about a topic as sensitive as cyber security.
- Registered charities.
- Cyber security sector businesses – businesses active within the UK that provide products or services that enable the protection of internet connected systems and their users. This was defined by the cyber security sector taxonomy used to create the sector list (see below).

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

This year's approach to sampling for private sector businesses differs from last year. This year we moved from the Inter-Departmental Business Register (IDBR) to Market Location sample for private sector business sample. This is different to previous waves, but the move is based on a precedent set by the Cyber Security Breaches Survey. The rationale for this change was greater population coverage and better sample information from Market Location than from IDBR.

We have maintained the previous sample sources for the public sector (IDBR), charities (the charity regulator databases) and cyber security sector (the database generated for the sectoral analysis).

Our approved supplier, Sample Solutions, further enhanced all the sample frames by matching in relevant key decision maker contact names (e.g. for IT Directors or Chief Information Security Officers, or board members in smaller businesses) from sources such as the Companies House database, Google Places API, publicly available LinkedIn data and company websites. This was in

addition to the existing senior contact and email data on the Market Location and charity databases.

Public sector organisations sample frame and sample selection

The sample frame for public sector organisations was from the government's IDBR, which covers organisations, across the UK at the enterprise level. This is the main sample frame for government surveys of public sector organisations. In total, we requested a random sample of 3,000 enterprises.

The inclusion/exclusion criteria for the public sector sample were as follows:

- Include all the UK (England, Wales, Scotland and Northern Ireland).
- Include public sector sample across all other sectors except education, public administration/defence, and health/social care. This is because there are a small proportion of public sector organisations outside these sectors which we do not want to systematically exclude.
- Exclude any legal statuses 1-3 (i.e. companies including building societies and partnerships).
- Exclude any enterprises with 0 or 1 employees at the enterprise level.
- Exclude enterprises with names including "parish council", "town council" or "community council".

Private sector businesses sample frame and sample selection

Records were selected 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 as this 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+)
- Education, finance or insurance businesses (which DSIT has highlighted as important sectors)
- Health, social care or social work businesses (which a 2018 literature review suggested was a sector with a greater demand for cyber security skills)
- Information or communication businesses (which are highly engaged with cyber security, according to CSBS findings)

Table 2.1 breaks down the originally selected sample by size and sector. As the survey outcomes later in this chapter show, only 11,498 market location 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 Market Location sample received by size and sector

SIC 2007 letter	Sector description	Micro (3 - 10)	Small (11 - 50)	Medium (51 - 250)	Large (251+)	Total
A	Agriculture, forestry and fishing	243	22	13	38	316
B, D, E	Utilities or production (excluding manufacturing)	26	14	22	75	137
C	Manufacturing	327	164	449	762	1,702
F	Construction	1,279	130	61	99	1,569
G	Wholesale and retail trade; repair of motor vehicles	989	222	175	421	1,807
H	Transportation and storage	283	36	46	225	590
I	Accommodation and food service activities	902	229	118	159	1,408
J	Information and communication	445	152	485	281	1,363
K	Financial and insurance activities	531	165	780	417	1,893
L	Real estate activities	250	50	23	78	401
M	Professional, scientific and technical	600	98	163	290	1,151
N	Administrative and support service acti	570	105	145	398	1,218
P	Education	355	104	104	325	888
Q	Human health and social work activities	398	257	585	756	1,996
R	Arts, entertainment and recreation	88	21	22	31	162
S	Other service activities	356	21	24	1	402
	Total	**7,642**	**1,790**	**3,215**	**4,356**	**17,003**

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/download-the-scottish-charity-register/
- The Charity Commission for Northern Ireland database: https://www.charitycommissionni.org.uk/charity-search/

This approach is consistent with all the previous waves of the Cyber Security Skills Study.

In England and Wales, and in Scotland, the respective charity regulator databases contain a comprehensive list of registered charities. The Charity Commission in Northern Ireland database has been established for several years now but is still in the process of registering missing charities to make the database more comprehensive.

Therefore, while the Charity Commission for 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.

As per previous years, DSIT 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 197 (see Table 2.2 for comparison with previous waves). 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.

Table 2.2: Number of charity interviews by wave

Report	Number of interviews
2025 report	197
2024 report	190
2023 report	214
2022 report	211
2021 report	220
2020 report	201
2018 report	470

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 1,178 charities to achieve 197 interviews.

Cyber security sector sample frame and sample selection

For cyber security sector businesses, the sample frame uses the 2,165 cyber security businesses identified in the DSIT 2025 Cyber Security Sectoral Analysis Report. From this database, there were 1,919 records with telephone numbers. A further 246 had email addresses only but were still included in the online survey invites via email.

All relevant 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 209 interviews.

Sample telephone and email tracing and cleaning for IDBR public sector sample

Not all of the original 2,893 cases of IDBR public sample were usable. In total, 391 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.

In keeping with the research conducted in 2023, to improve telephone coverage and response rates, we carried out automated telephone matching through the DBS Data business database as well as the Dun and Bradstreet business database for the IDBR public sector sample. This was not required for the other sample types (private sector, cyber security sector and charities) as these samples already had valid numbers.

We also cleaned the IDBR public sector 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. Central Government Departments were also excluded with a manual search.

In the final sample there were 2,072 cases for the public sector.

Sample matching for cyber security sector sample

For the cyber security sector sample, we did a subsequent manual search for missing cyber security sector numbers on company websites.

Sample matching for charity sector sample

There was already very high telephone coverage for charities from England and Wales (88% with telephone numbers), Northern Ireland (87% with telephone numbers) and Scotland (80% with telephone numbers). These provided a surplus of usable sample and minimised the possibility of non-response bias. Therefore, no telephone matching was required for charities.

Sample matching for private sector sample

There was also high telephone coverage for the Market Location private sector sample with 97% of records with telephone numbers. This provided a surplus of usable sample and minimised the possibility of non-response bias. Therefore, no telephone matching was required for private sector sample.

Sample enhancement

All samples were enhanced with email addresses and key decision makers where possible.

This process, as well as extra telephone matching for the IDBR public sector and cyber security sector sample, helped to reduce the likelihood of non-response bias affecting the survey.

Table 2.3: Post-cleaning available Market Location sample by size and sector

SIC 2007 letter	Sector description	**Micro (3-10)**	**Small (11–50)**	**Medium (51-250)**	**Large (251+)**	**Total**
A	Agriculture, forestry and fishing	242	22	13	35	312
B, D, E	Utilities or production (excluding manufacturing)	26	14	22	69	131
C	Manufacturing	324	164	438	717	1,643
F	Construction	1,274	129	61	96	1,569
G	Wholesale and retail trade; repair of motor vehicles	979	219	172	397	1,767
H	Transportation and storage	282	36	44	207	569
I	Accommodation and food service activities	895	227	117	150	1,389
J	Information and communication	434	144	443	229	1,250
K	Financial and insurance activities	525	163	757	376	1,821
L	Real estate activities	250	50	21	72	393
M	Professional, scientific and technical	597	97	158	248	1100
N	Administrative and support service acti	566	104	143	370	1183
P	Education	353	104	99	231	787
Q	Human health and social work activities	393	250	567	557	1,767
R	Arts, entertainment and recreation	88	21	21	25	155
S	Other service activities	351	21	24	0	396
	Total	**7,579**	**1,765**	**3,100**	**3,779**	**16,223**

The usable leads for the survey were randomly allocated into separate sample batches for businesses and charities. Each batch included leads proportionately selected to incorporate sample targets and expected response rates by sector and size band using data from previous Ipsos surveys with these audiences and prior batches from the current survey. 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 Table 2.5 for the total sample loaded).

2.3 Piloting

We conducted pilot fieldwork between 31st July and 5th August 2024. This involved written feedback reports from all interviewers working on the project during fieldwork, and analysis of raw survey data including interview lengths and sample outcomes.

We carried out 104 live pilot telephone interviews among the 4 audiences for the study. Much of the questionnaire remained unchanged and existing questions did not have to be rerouted.

Following the live pilot, we only made minor changes to the questionnaire, such as changing wording to the introduction, Q29_TECHNICAL, Q29_HIGHTECHNICAL, Q30_MANAGERIAL, Q19b_BAMENUM, Q20c_BAMEPER, Q20xc_BAMESENIOR, Q47e_DIVERSEACTION. These 104 interviews were included in the final dataset, as the changes made were not sufficiently substantive to impact the comparability of findings between the pilot and the main fieldwork period.

2.4 Fieldwork

Multimode data collection

All live pilot interviews were by telephone, with the online option being available for the main fieldwork period.

In practical terms, the multimode methodology worked as follows:

- Organisations could complete the survey either online through a unique link they had received in an email from Ipsos or via telephone with an Ipsos interviewer.
- Where organisations requested more information before deciding to take part in a telephone interview, interviewers could send out further information in a 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 4 reminder emails to those that had not completed the survey.
- This year we also included an open link for cyber security sector businesses to fill out. Unlike the unique link, this link could be used by a number of different cyber security sector businesses to fill out the survey. However, we only gained 4 completes from this method after ineligible cases were removed.

Table 2.4 shows that around 4% of the achieved interviews in total were online. This represents a decrease from last year's Cyber Security Skills Study, in which 8% completed the survey online, but aligns with the 4% observed in the 2023 release.

Table 2.4: Interviews by data collection mode

	Businesses		Public sector		Charities		Cyber security sector		Total	
Mode	n	%	n	%	n	%	n	%	n	%
Telephone	1,036	98%	109	97%	186	94%	178	85%	1,508	96 %
Online	25	2%	2	2%	11	6%	31	15%	69	4%

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

DSIT 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 impact 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 this was only 4% 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.
- 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 accurately 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 31st July to 18th October 2024. In total, we completed 1,578 interviews, comprising:

- 1,061 businesses (excluding sole traders)
- 111 public sector organisations (excluding parish councils)
- 197 registered charities
- 209 cyber security sector businesses.

The average interview length was c.13 minutes for businesses, public sector organisations and charities and c.20 minutes for cyber security businesses.

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 security sector that identified themselves as sole traders with no other employees on the payroll would have been classed as ineligible. These were excluded as they would make up the overwhelming majority of business sample units if included, and as they would typically be excluded from large portions of the questionnaire, e.g. on staff training and recruitment. *Within* the cyber security sector, sole trader cyber security businesses were still eligible, in line with previous years of the Cyber Security Skills Study and Cyber Security Sectoral Analysis surveys.

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 Northern Ireland, both companies were considered eligible.

Franchisees operating under the same company name but at different trading addresses were each considered eligible as separate, independent respondents.

Random-probability approach and maximising participation

We adopted random-probability sampling and interviewing to minimise selection bias. The overall aim with this approach is to have a known outcome for every sample lead that is released. For this survey, we used a robust approach comparable to the previous iterations of this research:

- We called each sample lead either a maximum 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.
- Each sample lead 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.
- Respondents were also given the option to complete the survey online rather than over the phone.
- 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 further information.
- We had a study website and GOV.UK page to reassure respondents that this was a legitimate government survey. We also offered respondents a government cyber security help card. The help card included up-to-date government guidance (from the National Cyber Security Centre) for organisations on cyber security to encourage participation. This can be found at Appendix B.

Additional steps taken to secure sample

We also took several extra steps to improve the sample coverage and the response rate, including:

- Matching telephone numbers from IDBR public sector sample with automated matching and cyber security sector sample with manual matching where required (as noted in Section 2.2).
- 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.
- 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 4 reminder emails to loaded sample across the course of fieldwork. In total, 58% (across all the types of samples) of the released sample had an email address, although these were largely general information or enquiries email addresses for the organisation.
- 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.

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% of the interviews and confirmed the data entry on screen for these interviews.

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 2.5 shows the final outcomes, the unadjusted response rate[4] and the adjusted response rate[5] for businesses (Market Location sample), public sector (the IDBR sample), charities and cyber security businesses.

Table 2.5: Fieldwork outcomes and response rate calculations by sample type

Outcome	Businesses (Market Location sample)	Public sector (IDBR sample)	Charities	Cyber security sector
Total sample released	11,498	1,499	1,178	2,251
Completed interviews	1,061	111	197	209
Expected eligibility	88%	93%	91%	96%
Unadjusted response rate	9%	7%	17%	22%
Adjusted response rate	11%	15%	23%	28%

[4] This is: completed interviews / total sample released.
[5] 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.

Unadjusted response rates compared to previous years

The unadjusted response rate (URR) for the IDBR sample is similar to the Cyber Security Skills 2024 Report (7% in 2025 report vs. 10% in 2024 report). For charities (17% in 2025 report vs. 16% in 2024 report) and cyber security businesses (9% in 2025 report vs. 11% in 2024 report), the URR is also similar. Therefore, the survey has performed broadly in line with the past 2 years across all groups. This year was the first year we used Market Location sample for private businesses so we cannot compare the URR of 9% to the previous survey.

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 can only be directly compared to the figures in the 2024, 2023 and 2022 Cyber Security Skills Study reports and should not be directly compared to the ARRs published in previous years' technical reports. We have simplified the ARR calculation in the last 2 years to use a single percentage figure for estimated eligibility, applied to both the refusals and the working numbers with unknown eligibility. For retrospective comparison, the ARR for this year compared to previous reports is shown in Table 2.6.

Table 2.6: Adjusted response rate (ARR) by sample type

Outcome	Public sector (IDBR sample)	Charities	Cyber security sector
2025 report	15%	23%	28%
2024 report	13%	23%	14%
2023 report	11%	24%	14%
2022 report	12%	26%	23%

The higher response rate for cyber security businesses this year may be because we have merged the 2 surveys. In previous years, the Cyber Security Skills Study came after the Cyber Security Sectoral Analysis which negatively affected the response rate for the Cyber Security Skills Study.

This year was the first year we used Market Location sample for private businesses. Therefore, we cannot compare the ARR of 11% to the previous surveys.

As this is the seventh year that we have contacted this sample, it is likely that there is a degree of survey fatigue. 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.[6]

2.5 Data processing and weighting

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

For business size, 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. For charities we used income band from the sample.

[6] 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).

Data management

The dataset was quality checked and cleaned. This included:

- Routing checks on all questionnaire variables.
- Checks to ensure on all demographic variables were accounted for.
- Checks on derived scripting variables created for analytical purposes.
- Cleaning of variable names, variable labels and value labels.
- Sense checks on all variables.

Coding

The verbatim responses to unprompted but closed 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 – 5 or more responses– 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 verify SIC coding in the survey. Instead, we used the SIC 2007 codes that were already in the IDBR or Market Location sample to assign businesses to a sector for weighting and analysis purposes. This is the same approach that was used in the 2024 survey and has been tested and validated in previous surveys, such as DCMS’s Cyber Security Breaches Survey series.[7] The sector groupings used in the main report match those shown in Tables 2.1 and 2.2.

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

Weighting

For the Market Location, IDBR and charity samples, we applied Random Iterative Method weighting (RIM weighting) to account, where possible, for non-response bias, and to account for the disproportionate sampling by size, sector and income band. The intention was to make the final reported data representative of the actual UK business, public sector and charity populations. This matched the weighting approach from the 2024 Cyber Security Skills Study report.

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**, we used non-interlocking weights by size and sector, based on the population profile in the 2024 Department for Business and Trade (DBT) business population estimates. 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 2024 DBT 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 sectors, we created a fourth weighting scheme that merged the private and public sector population profiles from the 2024 DBT estimates.

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

- There was no disproportionate sampling for this survey sample, so corrective weights were not needed.
- There is no other reliable profile data on the sector.

Tables 2.7 and 2.8 show the unweighted and weighted profiles of private businesses and charities.

Table 2.7: Unweighted and weighted sample profiles for businesses (private sector only)*

	Unweighted	Weighted
Size (private sector)		
Micro or small (1–49 staff)	69%	87%
Medium (50–249 staff)	13%	2%
Large (250+ staff)	9%	1%
Sector		
Agriculture, forestry or fishing	2%	3%
Utilities or production (including manufacturing)	9%	6%
Construction	8%	12%
Retail or wholesale	10%	16%
Transport or storage	2%	3%
Food or hospitality	6%	9%
Information or communications	8%	5%
Finance or insurance	7%	2%
Administration or real estate	8%	11%
Professional, scientific or technical	8%	12%
Education	10%	2%
Health, social care or social work	10%	4%
Entertainment, service or membership organisations	4%	6%
Region		
East Midlands	6%	6%
Eastern	9%	8%
London	9%	8%
North East	3%	3%
North West	8%	8%
Northern Ireland	3%	2%
Scotland	10%	10%
South East	15%	15%
South West	8%	10%
Wales	5%	5%
West Midlands	7%	7%
Yorkshire and Humberside	7%	7%

* Public sector organisations made up approximately 9% of both the unweighted and weighted profiles. These are not shown in the table above. Figures may not sum to the same total due to rounding.

Table 2.8: Unweighted and weighted sample profiles for charities

	Unweighted	Weighted
Income band[8]		
£0 to under £100,000	37%	77%
£100,000 to under £500,000	24%	15%
£500,000 or more	39%	8%

Figures may not sum to 100% due to rounding.

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

Analysis using the SPSS dataset

The SPSS dataset will be available on the UK Data Service. We aim to make this available within 3 months of publication.

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 security workforce, rather than as a proportion of employers:

- Career pathways into cyber security roles within the cyber security sector (section 5.4 in the findings report)
- Distribution of the cyber security sector workforce by specialism (Figure 2.2)
- Diversity estimates in the cyber security sector (Figure 3.1)
- Staff turnover estimates in the cyber security sector (Section 2.2)

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 security sector vacancies that are hard-to-fill (Section 6.2)

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

Outliers

Individual outliers in the data can heavily affect these estimates. Therefore, there were 2 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 from the diversity estimates.

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 may not sum to exactly 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 quantitative survey, Ipsos conducted 50 qualitative in-depth interviews between September and November 2024. This included:

- 24 cyber security sector businesses
- 11 medium and large private and public sector organisations (5 with 50-249 employees, and 8 with 250+ employees)
- 5 investors
- 4 recruitment agents sampled from different recruitment agencies who specialised in cyber security recruitment
- 6 cyber security training providers

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 therefore have a greater need for cyber security skills.
- The sample of large organisations achieved in the quantitative survey is relatively small, so it was particularly important to explore this audience in the remaining research strands.

3.1 Sampling and recruitment

Cyber security sector businesses and large organisations

The cyber security businesses and other medium and large organisations were mostly recruited from the survey. Ipsos also used its contacts and recontact sample from the Cyber Security Breaches Survey 2025 to help secure interviews with large businesses. The sampling was purposive – Ipsos identified the best organisations to recruit based on their survey responses, with the following quotas applied:

- Cyber security businesses that had recruited cyber security roles in the last 21 months or not
- Cyber security businesses who had had employees leave in the last 21 months or not
- Cyber security businesses that provided cyber security products, services or a mix
- Non-cyber security organisations required high-level technical cyber security skills and/or outsourced high-level technical cyber security skills
- Non-cyber security organisations that outsourced cyber security tasks or not, including outsourcing outside the UK

We also applied broader quotas to ensure a mix of organisations by sector and region (and by size within the cyber security sector, where recruitment was not restricted to just larger organisations). For medium sized private and public sector organisations, we only included those with at least 2 in their cyber security team and who do not outsource their high-level technical cyber security skills.

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 £70 thank you payment or charity donation if the participant was from the recontact sample or £100 if they were not from this sample to encourage participation.

Recruitment agents, training providers and investors

We sampled recruitment agents mainly through desk research, using online sources such as LinkedIn and recruitment agency websites to identify people recruiting for cyber security roles that

might be suited to the research. For training providers and investors, we used desk research and we received leads from Perspective Economics for these contacts.

We approached these potential participants via email. Upon them agreeing to take part, we initiated contact through email and asked further screener questions, to ensure they were eligible and guide the subsequent interview.

We offered a £100 thank you payment or charity donation to recruitment agents, investors and training providers, with the higher incentive 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 DSIT. Ipsos wrote these up in topic guides for each audience that DSIT approved for use. The full topic guides for each audience are included in Appendices C, D, E, F and G.

As a summary, the topics covered in the **cyber security firm** interviews included:

- Trends in customer demand
- Growth areas, emerging opportunities in cyber security
- Access to and demand for talent
- Outsourcing (asked to managed service providers only)
- Diversity of labour market
- Entry-level pathways and expectations
- Cyber Career Framework and UK Cyber Security Council's professional standards
- Future skills and training needs

The topics covered in the cyber security leads at **private and public sector organisations** were:

- Access to and demand for talent
- AI cyber security skills
- Entry-level pathways and expectations
- Cyber Career Framework and UK Cyber Security Council's professional standards
- Outsourcing
- Diversity of labour market
- Future skills and training needs

The topics covered in the **recruitment agent** interviews were:

- Trends in customer demand
- Labour market health and trends
- Diversity of labour market
- Entry-level pathways and expectations
- Cyber Career Framework and UK Cyber Security Council's professional standards
- Growth areas, emerging opportunities in cyber security

The topics covered in the **training providers** interviews were:

- Trends in customer demand
- Entry-level pathways and expectations
- Cyber Career Framework and UK Cyber Security Council's professional standards

- Diversity of labour market
- Growth areas, emerging opportunities in cyber security
- New and emerging training areas

The topics covered in the **investor** interviews were:

- Investor sentiment
- Growth enablers for sector
- Growth areas, emerging opportunities in cyber security

3.3 Analysis

To ensure rigorous thematic analysis, all interviews were recorded with participant consent and transcribed verbatim. Throughout the fieldwork, the core research team had regular discussions to analyse interim findings and identify key areas of focus in subsequent interviews. Two formal analysis sessions were conducted with DSIT, the first during fieldwork and the second after completion of fieldwork.

The transcribed data was then summarised and organised within an Excel framework, categorised by topic area of corresponding research questions. This structured approach facilitated systematic coding and thematic analysis of the interview data. Initial topic areas were derived from the topic guide headings and refined iteratively through reviewing categorised interview data within the Excel framework and insights gained from the analysis sessions. For example, the topic area 'diversity of the labour market' was further refined into sub-themes such as 'understanding of diversity', 'recruitment strategies for a more diverse cyber workforce', and 'challenges in improving diversity'. These refined themes were supported by illustrative, anonymised quotes and examples from the interview data. This process enabled identification of key themes and patterns within the Excel framework and ensured that selected quotes accurately reflected the overall key findings. Comprehensive summaries of each topic area, synthesising insights from the refined themes, were compiled to provide clear representations of key insights and overarching patterns in the data.

Job vacancies analysis

Perspective Economics led on the job vacancies analysis. 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 2024 calendar year (1st January to 31st December 2024). Across this report and the previous studies, 9 years of trend data have been examined (2016-2024 inclusive).

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

3.4 Methodology

Lightcast Analyst definition of cyber security job roles

Lightcast Analyst is a labour vacancy tool which provides data regarding job postings, occupations, specific industries and demographics. We have used 2 searches, analysing both core cyber security vacancies, and wider demand for cyber security skills across all roles.

Identifying core cyber security vacancies:

- Within the Lightcast tool, our search strategy for **core cyber security vacancies** is undertaken by identifying roles that request cyber security skills, with a focus on job titles such as "cyber security analysts" and "security architects" (see Appendix H for full list of search terms). For this analysis, we exclude over 80 occupations and 40 job titles that may request cyber security skills, but are not necessarily cyber specific roles, such as "financial managers" and "accountants". The report builder allows us to specify skills and qualifications that may be required in core cyber security positions.
- Core cyber security vacancies have been 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".

Identifying all vacancies requesting cyber security skills:

- Within the Lightcast tool, our search strategy for these vacancies explores job postings with cyber security skills and qualifications listed as a requirement. This search is set out in Appendix H.
- These 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".

Ensuring consistency across studies

The data used for this study is in line with the previous year's study (report published in 2024), replicating the Lightcast Analyst search strategy. We are therefore confident that our search strategy is well aligned to previous years.

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 removed trainee positions whereby there is no clear known employer, e.g. an advertisement for a cyber security training programme with no known job outcome.

Strengths to this approach

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 hundreds of thousands job postings over several years, exploring the specific jobs, skills, and qualifications in demand. It can also drill down into areas such as the specific coding languages being sought. This method can uncover geographic clustering (down to specific towns and cities) of high demand and skills shortages for cyber security professionals.
- **Real-time analysis** – the highly up-to-date data on Lightcast 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 Lightcast platform scrapes more than 40,000 online data sources. Online postings reflect the majority of job adverts, an estimated 85% of jobs posted in the labour market, compared to other sources such as print media.

Limitations to this approach

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

- **Selection bias** – Lightcast typically 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 Lightcast interpretation of cyber security jobs is reliant upon their definition, based on the skills, job titles and qualifications expected for cyber security roles. There is a risk that some roles within their interpretation may not truly be considered a cyber security 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 adopted a more bespoke search strategy, with the tailored inclusion/exclusion terms. These search terms reduce the risk of including non-cyber security roles (false positives) within the analysis.

3.5 Metrics analysed

The analysis explores the following data outputs from the Lightcast 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 employers and sectors advertising the largest number of cyber security vacancies.
- 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 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).

3.6 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 Lightcast 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).

4 Supply side analysis

Perspective Economics led this strand of the research. It replicated the methodology used in the previous year's study (report published in 2024), 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 2024/25). 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 security workforce gap (i.e. the annual shortfall of people working in cyber security roles)

4.1 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	2023/24 academic year (apprenticeships), and 2021/22 (further education)
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)	2022/23 academic year
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	2021/22 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	Perspective Economics estimates based on	UK-wide	2024 estimate (certain data unchanged

Type	Metrics	Source	UK region covered	Time period covered
	▪ Certification data	updated certification data, where available		since the previous report)
Estimation of outflows	▪ Retirement and other reasons for leaving the cyber security business within last 12 months	Ipsos estimate based on the survey of cyber security businesses	UK-wide	Survey fieldwork undertaken in late 2024

4.2 Cyber security workforce gap calculation

The calculation of the cyber security 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 9 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 an estimate for the size of the current cyber security recruitment pool. We have taken the estimated cyber security workforce from the Cyber Security Skills Study (report published in 2024) of c.136,800, and applied the estimated inflows and outflows set out within this year's report (i.e. approximately 9,100 new entrants, and a further 2,600 moving into the sector from aligned professions, and approximately 5,500 exiting the sector last year). This suggests an estimated current cyber security workforce figure of c.143,000 (at the start of 2025).

We then apply the 5% growth rate (conservative estimate) in Full Time Equivalents (FTEs) from the Cyber Security Sectoral Analysis 2024, to estimate the additional annual demand for the twelve-month period. This suggests that, assuming a 5% growth rate, the ecosystem could demand approximately 7,200 new individuals.

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 (2022/23) data on people graduating from higher education courses in cyber security.
- The latest (2022/23) data on people graduating from higher education courses in computer science.
- The latest (2023/24) data on people completing relevant apprenticeships.
- 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).

We estimate an inflow of approximately 9,100 people per annum into the UK cyber security workforce.

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 security sector (covered in Chapter 9 of the findings report) and extrapolate this to the entire cyber security workforce (within and outside the cyber security sector). Applying this survey estimate (3.5%) to our estimate for the size of the current cyber security recruitment workforce (143,000), we calculate the expected number of people who may leave the cyber security workforce in 2025 (c.5,700 persons).

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 security sector. In practice, not all the FTEs within the cyber security sector are people working in cyber security roles. They will also include a number of people in non-cyber security roles (e.g. in diversified companies that offer cyber security and non-cyber security 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 potential demand for 2025, we have assumed that the growth rate of the cyber security workforce in 2025 will be approximately 5% (in line with the workforce estimates between 2024 and 2025 in this report). We note this is lower than the ‘sectoral’ estimates in the 2025 DSIT Cyber Security Sectoral Analysis; however, this is informed by the workforce level estimates and wider qualitative findings set out in this skills research.

5 Research burden

The Government Statistical Service (GSS) has a policy of monitoring and reducing statistical survey burden to participants where possible, and the burden imposed should be proportionate to the benefits arising from the use of the statistics. As a producer of statistics, DSIT is committed to monitoring and reducing the burden on those providing their information, and on those involved in collecting, recording and supplying data.

This section calculates the research compliance cost, in terms of the time cost on respondents, imposed by both the quantitative survey and qualitative fieldwork.

- The quantitative survey had 1,578 respondents and the average (mean) survey length was c.14 minutes. Therefore, the research compliance cost for the quantitative survey this year was [1,578 × 14 minutes = 368 hours]. This breaks downs as follows (total may not sum exactly due to rounding):
  - The average (mean) survey length was c. 13 minutes for businesses, public sector organisations and charities, i.e. [1,369 x 13 minutes = 297 hours].
  - The average (mean) survey length was c. 20 minutes for cyber security sector businesses, i.e. [209 x 20 minutes = 70 hours].
- The qualitative research had 50 respondents, and the average interview length was 60 minutes. The research compliance cost for the qualitative strand this year was [50 × 60 minutes = 50 hours].

In total, the compliance cost for the Cyber Security Sectoral Analysis and Cyber Security Skills Study project (published in 2025) was approximately 418 hours.

Appendix A: 2025 report questionnaire

Key

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

Introduction

SHOW IF TELEPHONE RESPONDENT (MODETYPE=CATI)
CATIINTRO
Is this the head office for [S_CONAME]?

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

Hello, my name is … from Ipsos, the independent research organisation.

S_FREENUMTEXT

Ipsos and its partner, Perspective Economics, are conducting a survey on behalf of the UK Government Department for Science, Innovation and Technology. It's about [S_CYBERTEXTA].

S_CYBERTEXTB

We are not trying to sell you anything.

S_RESPTEXT
Would you be happy to take part in an interview this year?

S_LENGTHTEXT

S_INCENTIVETEXT

ADD EXTRA SOFT INCENTIVE FOR SMALLER ORGANISATIONS IF NECESSARY:

- As a thank you, we can send you a government help card with the latest official cyber security guidance for organisations. This would get emailed to you as soon as you complete the survey.

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-sector-and-labour-market
- You can also Google the term "Understanding the UK cyber security sector and labour market" to find the same link yourself.

SHOW IF ONLINE RESPONDENT (MODETYPE=WEB/ONLINE)
INTROSCREEN
Thank you for taking part in this confidential Ipsos and Perspective Economics survey.

IF OPEN ONLINE LINK RESPONDENT (SCRIPTER TO DEFINE): For the first 220 cyber sector businesses to complete the survey, either online or via a telephone interview, we will make a £20 charity donation to Code your Future, or another charity you choose from our list at the beginning of the survey.

IF NON-CYBER SECTOR (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 (S_TYPE=3): This survey should be completed by a senior person responsible for the growth, skills and recruitment needs of your cyber business.

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 https://www.gov.uk/government/publications/understanding-the-uk-cyber-security-sector-and-labour-market. 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 (MODETYPE=CATI)
REASSURANCE_EMAIL
READ OUT IF TELEPHONE RESPONDENT (MODETYPE=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 OPEN ONLINE LINK RESPONDENT (SCRIPTER TO DEFINE)
VALIDATION
Ipsos is also directly emailing and calling businesses to take part in this research. We want to ensure we do not contact you again if you have already completed the survey via this link. For that, we just need to confirm **either** your registered business name **or** your business website.

SINGLE CODE
1. Registered business name WRITE IN
2. Business website WRITE IN

ASK IF TELEPHONE RESPONDENT (MODETYPE=CATI)
Q1w_CONSENTA
Before we start, I just want to clarify that participation in the survey is confidential and voluntary. Results will be anonymised and not attributable to you. You can change your mind at any time.

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 the gov.uk website at: https://www.gov.uk/government/publications/understanding-the-uk-cyber-security-sector-and-labour-market

SINGLE CODE
1. Yes
2. No

CODE 2 CLOSES SURVEY

ASK IF ONLINE RESPONDENT (MODETYPE=WEB/ONLINE)

Q1x_ONLINERESP

IF NON-CYBER SECTOR (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 (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

1. Yes – a senior person
2. No

CODE 2 CLOSES SURVEY ("Thank you for your interest in this survey. Please pass the email link to this survey to the relevant senior individual in your organisation.")

Q1y_CONSENTC DELETED IN 2025 QUESTIONNAIRE

Q1z_CONSENTCDUM DELETED IN 2025 QUESTIONNAIRE

ASK IF SAMPLED AS LARGE BUSINESS (S_TYPE=1 AND S_SIZEBAND=4) OR CYBER SECTOR (S_TYPE=3)

Q48x_INCENTIVE

IF OPEN ONLINE LINK RESPONDENT (SCRIPTER TO DEFINE): If you are one of the first 220 cyber sector businesses to complete this survey:

We will make a [IF LARGE BUSINESS (S_TYPE=1 AND S_SIZEBAND=4): £15/IF CYBER SECTOR (S_TYPE=3): £20] charity donation on your behalf as a thank you for taking part. We have three charities for you to choose from:

- Code your Future
- Mind
- Turn2us

ADD IF NECESSARY:

- Code your Future offers coding courses to refugees and other disadvantaged individuals
- Mind is a mental health charity offering information and advice to people with mental health problems, and campaigning on their behalf
- Turn2us helps people in financial need gain access to charitable grants and other financial help

PROMPT TO CODE

SINGLE CODE

1. Code your Future
2. Mind
3. Turn2us
4. DO NOT READ OUT: I do not want Ipsos to make a charity donation on my behalf

ASK IF SAMPLED AS SME (S_TYPE=1 AND S_SIZEBAND=1-3) OR CHARITY (S_TYPE=2)

Q49_HELPCARD

Would you like us to email you a government help card, with links to the latest official cyber security guidance for organisations? We can collect your email at the end of the interview.

SINGLE CODE

1. Yes
2. No

ASK IF CYBER SECTOR (S_TYPE=3)

Q28a_LINK

In order to ensure the best use of your survey results, Ipsos and Perspective Economics would like to link your answers to other publicly available data about your business, in areas like employment and turnover, as well as any survey responses from last year.

Are you happy for us to link your answers to these records? This is for statistical analysis purposes only.

SINGLE CODE

1. Yes
2. No

Organisation size (both cyber sector and outside cyber sector)

Q1_TYPEX DELETED IN 2025 QUESTIONNAIRE

Q1a_TYPEXDUM DELETED IN 2025 QUESTIONNAIRE

ASK ALL

Q2_SIZEA

IF PRIVATE SECTOR OR CYBER SECTOR (S_TYPE=1 OR 3):

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.

IF CHARITY (S_TYPE=2):

Including yourself, how many employees, volunteers and trustees 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 people who regularly volunteer for your organisation in the UK. This does not include operations outside the UK.

IF LOCAL AUTHORITY (S_LASTATUS=1-2):

Including yourself, how many employees and council members are there in your organisation?

IF OTHER PUBLIC SECTOR (S_LASTATUS≠1-2 AND S_TYPE=4):

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

SINGLE CODE

1. WRITE IN RANGE 2 TO 99,999 (SOFT CHECK IF >9,999, “Did you say [ANSWER]?”)
2. IF WEB: I am the sole trader CLOSE SURVEY IF NOT CYBER SECTOR (S_TYPE≠3)
3. IF CATI: Respondent is sole trader CLOSE SURVEY NOT CYBER SECTOR (S_TYPE≠3)
4. DO NOT READ OUT: Don’t know

ASK IF DON’T KNOW SIZE OF ORGANISATION (SIZEA CODE DK)

Q3_SIZEB

IF PRIVATE SECTOR OR CYBER SECTOR (S_TYPE=1 OR 3):

Which of these best represents the number of employees working in your organisation across the UK as a whole, including yourself?

IF CHARITY (S_TYPE=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?

IF LOCAL AUTHORITY (S_LASTATUS=1-2):
Which of these best represents the number of employees and council members in your organisation, including yourself?

IF OTHER PUBLIC SECTOR (S_LASTATUS≠1-2 AND S_TYPE=4):
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

1. Under 10
2. 10 to 49
3. 50 to 249
4. 250 to 499
5. 500 to 999
6. 1,000 or more
7. 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 SIZEA AND SIZEB

1. Under 10
2. 10 to 49
3. 50 to 249
4. 250 to 499
5. 500 to 999
6. 1,000 or more
7. Don't know

Q4_SALESA DELETED IN 2025 QUESTIONNAIRE

Q5_SALESB DELETED IN 2025 QUESTIONNAIRE

Q5a_SALES DELETED IN 2025 QUESTIONNAIRE

Q6_DEFINE DELETED POST-PILOT IN 2018 QUESTIONNAIRE

Outsourcing (outside cyber sector)

ASK IF NOT CYBER SECTOR (S_TYPE≠3)

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.

SINGLE CODE

1. Yes

2. No
3. DO NOT READ OUT: Don't know

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND OUTSOURCE (OUTSOURCE CODE 1)

OUTSOURCEINTRO

We'd now like to ask a few more questions about this outsourcing.

Q8_HOWMUCH DELETED IN 2020 QUESTIONNAIRE

Q9_REASONOUT DELETED IN 2020 QUESTIONNAIRE

Q10_INVESTOUT DELETED POST-PILOT IN 2018 QUESTIONNAIRE

Q11_INVESTOUTB DELETED POST-PILOT IN 2018 QUESTIONNAIRE

Q12_OUTVALUES DELETED POST-PILOT IN 2018 QUESTIONNAIRE

ASK IF OUTSOURCE (OUTSOURCE CODE 1)

Q13_WHATOUT

Which of the following aspects of cyber security are covered by your outsourced provider or providers?
READ OUT

ASK AS A GRID IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB
RANDOMISE STATEMENT ORDER BUT KEEP i LAST (EVEN IF NEW STATEMENTS ADDED IN LATER WAVES)

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 or vulnerability scanning
    - using threat intelligence tools
    - forensic analysis
    - interpreting malicious code
    - autonomous cyber defences
    - or using tools to monitor user activity
j. An external Security Operations Centre
k. Setting up new user accounts and authentications securely

SINGLE CODE

1. Yes, outsourced
2. No, not outsourced
3. DO NOT READ OUT: Don't know

ASK IF OUTSOURCE HIGHER-LEVEL FUNCTIONS (WHATOUT i 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 IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB
RANDOMISE STATEMENT ORDER

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
g. Carrying out vulnerability scans
h. Any autonomous cyber defences

SINGLE CODE

1. Yes
2. No
3. DO NOT READ OUT: Don't know

ASK IF OUTSOURCE (ANY WHATOUT CODE 1)

Q14a_WHATOUTNONUK

Do you outsource any of the following to individuals or organisations outside the UK?

SHOW ONLY STATEMENTS WHERE WHATOUT a-k CODE 1
ASK AS A GRID IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB
RANDOMISE STATEMENT ORDER BUT KEEP i LAST (EVEN IF NEW STATEMENTS ADDED IN LATER WAVES)

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 or vulnerability scanning
    - using threat intelligence tools
    - forensic analysis
    - interpreting malicious code
    - autonomous cyber defences
    - or using tools to monitor user activity
j. An external Security Operations Centre
k. Setting up new user accounts and authentications securely

SINGLE CODE

1. Yes
2. No
3. DO NOT READ OUT: Don't know

ASK IF OUTSOURCE MORE THAN ONE HIGHER-LEVEL FUNCTION (MORE THAN ONE WHATHIGHER a-h CODE 1) AND OUTSOURCE HIGHER-LEVEL FUNCTIONS OUTSIDE UK (WHATOUTNONUK i CODE 1)

Q14b_WHATHIGHERNONUK

Which of the following specific higher-level functions do you outsource outside the UK?
READ OUT

SHOW ONLY STATEMENTS WHERE WHATHIGHER a-h CODE 1
ASK AS A GRID IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB
RANDOMISE STATEMENT ORDER

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
g. Carrying out vulnerability scans
h. Any autonomous cyber defences

SINGLE CODE

1. Yes
2. No
3. DO NOT READ OUT: Don't know

DUMMY VARIABLE NOT ASKED
Q14c_WHATHIGHERNONUKDUM
Higher-level functions outsourced outside the UK:

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
g. Carrying out vulnerability scans
h. Any autonomous cyber defences

SINGLE CODE

- IF OUTSOURCE MORE THAN ONE HIGHER-LEVEL FUNCTION (MORE THAN ONE WHATHIGHER a-h CODE 1) AND OUTSOURCE HIGHER-LEVEL FUNCTIONS OUTSIDE UK (WHATOUTNONUK i CODE 1), TAKE ANSWER FROM WHATHIGHERNONUK
- IF OUTSOURCE ONE HIGHER-LEVEL FUNCTION (ONE WHATHIGHER a-h CODE 1, TAKE ANSWER FROM WHATHIGHER)
- ELSE MISSING

Q15.DEALINGOUT DELETED IN 2020 QUESTIONNAIRE

Q16.PERFORMOUT DELETED POST-PILOT IN 2018 QUESTIONNAIRE

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND NOT CYBER SECTOR (S_TYPE≠3)
WORKFORCEINTRO
Now I'd like to ask some questions about you and others **within** your organisation who 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.]

SHOW IF ONLINE RESPONDENT (MODETYPE=WEB/ONLINE) AND NOT CYBER SECTOR (S_TYPE≠3)
WORKFORCESCREEN
The following questions are about you and others **within** your organisation who 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.]

Workforce size and profile (cyber sector)

Q16a.TITLE DELETED IN 2021 QUESTIONNAIRE

Q17_TEAM DELETED IN 2025 QUESTIONNAIRE

ASK IF CYBER SECTOR (S_TYPE=3) AND NOT SOLE TRADER (SIZEA NOT CODES 2-3)
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

SINGLE CODE
1. WRITE IN RANGE 1 TO SIZEA OR TOP END OF SIZEB, OTHERWISE 99,999 ((SOFT CHECK IF >9,999, "Did you say [ANSWER]?")
2. 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. 1 to 4
2. 5 to 9
3. 10 to 29
4. 30 to 49
5. 50 to 249
6. 250 to 499
7. 500 to 999
8. 1,000 or more
9. DO NOT READ OUT: Don't know

DUMMY VARIABLE NOT ASKED
Q17c_CYBERSIZEDUM
How many of your employees are working in cyber security roles?

SINGLE CODE, MERGE RESPONSES FROM CYBERSIZE, AND SIZEA IF SOLE TRADER
1. WRITE IN RANGE 1 TO 99,999 (WHERE SIZEA CODES 2-3=1)
2. 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 CYBERSIZE AND CYBERSIZEB, AND SIZEA IF SOLE TRADER (WHERE SIZEA CODES 2-3 BECOME CODE 1 HERE)
1. 1 to 4
2. 5 to 9
3. 10 to 29
4. 30 to 49
5. 50 to 249
6. 250 to 499
7. 500 to 999
8. 1,000 or more
9. Don't know

Q18_PATHWAY DELETED IN 2025 QUESTIONNAIRE

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.

SINGLE CODE
1. WRITE IN RANGE 1 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM (HARD CHECK IF TOTAL >CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM, "You said you only had [CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM] employees in cyber roles.")
2. 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
- ELSE MERGE RESPONSES FROM CYBERSENIOR

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1-3)
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

SINGLE CODE
1. WRITE IN RANGE 0 TO CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM FOR EACH STATEMENT (HARD CHECK IF TOTAL ACROSS STATEMENTS = 0, OR IF TOTAL ACROSS STATEMENTS > (CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM), "You said you only had [CYBERSIZEDUM OR TOP OF CYBERSIZEBDUM] employees in cyber roles.")
2. DO NOT READ OUT: Don't know

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4-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 IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB
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
1. None of them
2. Under a quarter
3. More than a quarter, under a half
4. More than a half, under three-quarters
5. More than three-quarters, but not all
6. All of them (i.e. 100%)
7. DO NOT READ OUT: Don't know

Barriers to growth (cyber sector)

ASK IF CYBER SECTOR (S_TYPE=3)
Q20_BARRIERS
To what extent, if at all, have any of the following issues affected your ability to meet your business goals across the last 12 months?
READ OUT

RANDOMISE ORDER OF SETS OF STATEMENTS AND ORDER WITHIN SETS OF STATEMENTS
ASK ON SEPARATE SCREENS IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB

SET 1
a. A lack of candidates in the labour market that have the technical cyber security skills that you need
b. A lack of candidates in the labour market that have non-technical skills, such as communication, leadership, management or sales and marketing skills

SET 2
c. Your existing employees lacking the technical cyber security skills that you need
d. Your existing employees lacking non-technical skills, such as communication, leadership, management or sales and marketing skills

SET 3
e. Competition for candidates from other businesses in the cyber sector
f. Competition for candidates from other businesses **outside** the cyber sector

SET 4
g. Salary demands of candidates not being affordable
h. Staff moving jobs or retiring

SINGLE CODE, REVERSE SCALE
1. To a great extent
2. To some extent
3. Not very much
4. Not at all
5. DO NOT READ OUT: Don't know

UK Cyber Security Council awareness (cyber sector)

ASK IF CYBER SECTOR (S_TYPE=3)
Q18x_COUNCILAWARE
The UK Cyber Security Council is the self-regulatory body for the UK's cyber security profession. Before this interview, had you heard of the UK Cyber Security Council?

SINGLE CODE
1. Yes
2. No
3. DO NOT READ OUT: Don't know

Cyber security specialisms (cyber sector)

Q18d_JOBROLENUM DELETED IN 2023 QUESTIONNAIRE

Q18e_JOBROLEPER DELETED IN 2023 QUESTIONNAIRE

Q18f_WEBSITE DELETED IN 2025 QUESTIONNAIRE

ASK IF CYBER SECTOR (S_TYPE=3)
Q18g_JOBROLE
IF TELEPHONE RESPONDENT (MODETYPE=CATI): For the next questions, we would like you to look at the UK Cyber Security Council's 16 cyber security specialisms online. You can Google "Cyber Career Framework", or I can give you the exact weblink. You will need to scroll down the page to see the 16 specialisms.

If needed, you can click on each specialism to bring up a brief description of it, but you don't need to click on the "Learn More" button to answer this question.

ADD IF NECESSARY: https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Which **one** of these cyber security specialisms would you say best describes your role?
IF MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1): Do any of the employees working in cyber security roles, including you, specialise in any of these roles? You can give an answer for each individual working in a cyber security role.

ADD IF NECESSARY: If you are a generalist or work across multiple areas, a specialism would be the area in which you spend most of your time in this role. If there is an equal split, it is the area where you have the deepest knowledge or experience.

ADD IF NECESSARY: If you primarily manage and oversee cyber security operations, or lead an organisation or team, rather than performing detailed technical work, please select **Cyber Security Management**.
DO NOT READ OUT

MULTICODE UP TO CYBERSIZEDUM (ERROR MESSAGE FOR WEB: "You said you had [CYBERSIZEDUM] person/people working in cyber roles in total.")
REVERSE ORDER FOR WEB (NOT CATI), EXCEPT CODE 16

1. **Cryptography and Communications Security** – the designing, development, testing, implementation and operation of a system or product to provide cryptographic or secure communications
2. **Cyber Security Audit and Assurance** – the verification that systems and processes meet the specified security requirements and that processes to verify on-going compliance are in place
3. **Cyber Security Governance and Risk Management** – the monitoring of compliance with agreed cyber security policies and the assessment and management of relevant risks
4. **Cyber Security Management** – the management of cyber security resources, staff and policies at an enterprise level in line with business objectives and regulatory requirements
5. **Cyber Threat Intelligence** – the assessment, validation and reporting of information on current and potential cyber threats to maintain an organisation's situational awareness
6. **Data Protection and Privacy** – the management of the protection of data, enabling an organisation to meet its contractual, legal and regulatory requirements
7. **Digital Forensics** – the process of identifying and reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system
8. **Identity and Access Management** – the management of policies, procedures and controls to

ensure that only authorised individuals access information or computer-controlled resources
9. **Incident Response** – the preparation for, handling of and following up of cyber security incidents, to minimise the damage to an organisation and prevent recurrence
10. **Network Monitoring and Intrusion Detection** – the monitoring of network and system activity to identify unauthorised actions by users or potential intrusion by an attacker
11. **Secure Operations** – the management of an organisation's information systems operations in accordance with the agreed Security Policy
12. **Secure System Architecture and Design** – the designing of an IT system to meet its security requirements, balancing this with its functional requirements
13. **Secure System Development** – the development and updating of a system or product, in conformance with agreed security requirements and standards, throughout its lifecycle
14. **Security Testing** – the testing of a network, system, product or design, against the specified security requirements and/or for vulnerabilities (penetration testing)
15. **Vulnerability Management** – the management of the configuration of protected systems to ensure that any vulnerabilities are understood and managed
16. **Another area**

SINGLE CODE

17. DO NOT READ OUT: Don't know

ASK IF HAVE TECHNICAL SKILLS ISSUES AT LEAST TO SOME EXTENT (BARRIERSa OR BARRIERSc CODES 1-2)

Q21b_SPECIALISMS

IF TELEPHONE RESPONDENT (MODETYPE=CATI): For this question, please stay on the same weblink.

ADD IF NECESSARY: https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

You previously said you have had issues with cyber security skills, either among job candidates, or among your existing employees. In which of these specialisms, if any, would you say your business lacks the skills you need?

MULTICODE

REVERSE ORDER FOR WEB (NOT CATI), EXCEPT CODE 16

1. **Cryptography and Communications Security** – the designing, development, testing, implementation and operation of a system or product to provide cryptographic or secure communications
2. **Cyber Security Audit and Assurance** – the verification that systems and processes meet the specified security requirements and that processes to verify on-going compliance are in place
3. **Cyber Security Governance and Risk Management** – the monitoring of compliance with agreed cyber security policies and the assessment and management of relevant risks
4. **Cyber Security Management** – the management of cyber security resources, staff and policies at an enterprise level in line with business objectives and regulatory requirements
5. **Cyber Threat Intelligence** – the assessment, validation and reporting of information on current and potential cyber threats to maintain an organisation's situational awareness
6. **Data Protection and Privacy** – the management of the protection of data, enabling an organisation to meet its contractual, legal and regulatory requirements
7. **Digital Forensics** – the process of identifying and reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system
8. **Identity and Access Management** – the management of policies, procedures and controls to ensure that only authorised individuals access information or computer-controlled resources
9. **Incident Response** – the preparation for, handling of and following up of cyber security incidents, to minimise the damage to an organisation and prevent recurrence
10. **Network Monitoring and Intrusion Detection** – the monitoring of network and system activity to

identify unauthorised actions by users or potential intrusion by an attacker

11. **Secure Operations** – the management of an organisation's information systems operations in accordance with the agreed Security Policy
12. **Secure System Architecture and Design** – the designing of an IT system to meet its security requirements, balancing this with its functional requirements
13. **Secure System Development** – the development and updating of a system or product, in conformance with agreed security requirements and standards, throughout its lifecycle
14. **Security Testing** – the testing of a network, system, product or design, against the specified security requirements and/or for vulnerabilities (penetration testing)
15. **Vulnerability Management** – the management of the configuration of protected systems to ensure that any vulnerabilities are understood and managed
16. **Another area**

SINGLE CODE

17. DO NOT READ OUT: None of these/no current skills needs
18. DO NOT READ OUT: Don't know

Q18j_GENERALIST DELETED IN 2025 QUESTIONNAIRE

Workforce diversity (cyber sector)

Q19_DIVERSITYA DELETED IN 2020 QUESTIONNAIRE

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND CYBER SECTOR (S_TYPE=3)
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 RESPONDENT (MODETYPE=WEB/ONLINE) AND CYBER SECTOR (S_TYPE=3)
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 1-3)
Q19a_FEMALENUM
IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Would you describe yourself as female?
IF MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1): 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.

SINGLE CODE

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

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1-3)
Q19b_BAMENUM
IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Would you describe yourself as being from an ethnic minority background?
IF MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1): How many are from ethnic minority backgrounds?
ADD IF NECESSARY: By "ethnic minority background", we mean not white or caucasian.
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

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

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1-3)

Q19x_DISABILITYNUM

IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Would you describe yourself as having a disability? That is, any long-standing illness, condition or impairment, which causes difficulty with day-to-day activities.

IF MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1): 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.

SINGLE CODE

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

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1-3)

Q19c_NEURONUM

IF ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM=1): Would you describe yourself as having any neurodiverse conditions or learning disorders, such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD)?

IF MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1): 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.

SINGLE CODE

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

Q20_DIVERSITYB DELETED IN 2020 QUESTIONNAIRE

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4-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.

SINGLE CODE

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

ASK IF CAN'T SAY EXACT PERCENTAGE (FEMALEPER CODE DK OR REF/PREFER NOT TO SAY/PREFER NOT TO SAY)

Q20b_FEMALEPERB

Is it…?

PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)

SINGLE CODE

1. None of them
2. Under a quarter
3. More than a quarter, under a half
4. More than a half, under three-quarters
5. More than three-quarters, but not all
6. All of them (i.e. 100%)
7. DO NOT READ OUT: Don't know
8. DO NOT READ OUT: Prefer not to say

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4-DK)

Q20c_BAMEPER

Roughly what proportion are from ethnic minority backgrounds?

PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)

ADD IF NECESSARY: By "ethnic minority background", we mean not white or caucasian.

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

1. None of them
2. Under a quarter
3. More than a quarter, under a half
4. More than a half, under three-quarters
5. More than three-quarters, but not all
6. All of them (i.e. 100%)
7. DO NOT READ OUT: Don't know
8. DO NOT READ OUT: Prefer not to say

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4-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

1. None of them
2. Under a quarter
3. More than a quarter, under a half
4. More than a half, under three-quarters
5. More than three-quarters, but not all
6. All of them (i.e. 100%)
7. DO NOT READ OUT: Don't know
8. DO NOT READ OUT: Prefer not to say

ASK IF LARGE CYBER SECTOR (CYBERSIZEBDUM CODES 4-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

1. None of them
2. Under a quarter
3. More than a quarter, under a half

4. More than a half, under three-quarters
5. More than three-quarters, but not all
6. All of them (i.e. 100%)
7. DO NOT READ OUT: Don't know
8. DO NOT READ OUT: Prefer not to say

DUMMY VARIABLE NOT ASKED
Q_DISADVDUM

MULTICODE
1. IF HAVE WOMEN IN CYBER ROLES ((FEMALENUM>0 OR FEMALEPER>0 OR (FEMALEPERB NOT CODE 1 OR DK OR REF/PREFER NOT TO SAY)): Have women in cyber roles
2. IF HAVE ETHNIC MINORITIES IN CYBER ROLES ((BAMENUM>0 OR (BAMEPER NOT CODE 1 OR DK OR REF/PREFER NOT TO SAY)): Have ethnic minorities in cyber roles
3. IF HAVE DISABLED PEOPLE IN CYBER ROLES ((DISABILITYNUM>0 OR (DISABLITYPER NOT CODE 1 OR DK OR REF/PREFER NOT TO SAY)): Have disabled people in cyber roles
4. IF HAVE NEURODIVERGENT PEOPLE IN CYBER ROLES ((NEURONUM>0 OR (NEUROPER NOT CODE 1 OR DK OR REF/PREFER NOT TO SAY)): Have neurodivergent people in cyber roles

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND HAVE ANY DISADVANTAGED GROUPS IN CYBER ROLES (DISADVDUM CODES 1-4) AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1) AND ANSWERED HOW MANY IN SENIOR CYBER ROLES (CYBERSENIORDUM≥1)
SENIORINTRO
On the same theme, these next questions focus on your [CYBERSENIORDUM] principal or director-level cyber staff.

SHOW IF ONLINE RESPONDENT (MODETYPE=WEB/ONLINE) AND HAVE ANY DISADVANTAGED GROUPS IN CYBER ROLES (DISADVDUM CODES 1-4) AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1) AND ANSWERED HOW MANY IN SENIOR CYBER ROLES (CYBERSENIORDUM≥1)
SENIORSCREEN
On the same theme, these next questions focus on your [CYBERSENIORDUM] principal or director-level cyber staff.

ASK IF HAVE WOMEN IN CYBER ROLES (DISADVDUM CODE 1) AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1) AND ANSWERED HOW MANY IN SENIOR CYBER ROLES (CYBERSENIORDUM≥1)
Q20xb_FEMALESENIOR
IF ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM=1): Is this principal or director-level staff member female?
IF MORE THAN ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM≠1): How many of the principal or director-level staff members are female?
ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

SINGLE CODE
1. WRITE IN RANGE 0 TO LOWEST OF FEMALENUM OR CYBERSENIORDUM (WARNING FOR WEB IF NOT WITHIN RANGE: Your answer cannot be more than the total number of director-level staff or of female employees in cyber roles.)
2. DO NOT READ OUT: Don't know
3. DO NOT READ OUT: Prefer not to say

ASK IF HAVE ETHNIC MINORITIES IN CYBER ROLES (DISADVDUM CODE 2) AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1) AND ANSWERED HOW MANY IN SENIOR CYBER ROLES (CYBERSENIORDUM≥1)

Q20xc_BAMESENIOR

IF ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM=1): Is this principal or director-level staff member from an ethnic minority background?

IF MORE THAN ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM≠1): How many of the principal or director-level staff members are from ethnic minority backgrounds?

ADD IF NECESSARY: By "ethnic minority background", we mean not white or caucasian.

ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

SINGLE CODE

1. WRITE IN RANGE 0 TO LOWEST OF BAMENUM OR CYBERSENIORDUM (WARNING FOR WEB IF NOT WITHIN RANGE: Your answer cannot be more than the total number of director-level staff or of ethnic minority employees in cyber roles.)
2. DO NOT READ OUT: Don't know
3. DO NOT READ OUT: Prefer not to say

ASK IF HAVE DISABLED MINORITIES IN CYBER ROLES (DISADVDUM CODE 3) AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1) AND ANSWERED HOW MANY IN SENIOR CYBER ROLES (CYBERSENIORDUM≥1)

Q20xd_DISABILITYSENIOR

IF ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM=1): Is this principal or director-level staff member disabled?

IF MORE THAN ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM≠1): How many of the principal or director-level staff members are disabled?

ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

SINGLE CODE

1. WRITE IN RANGE 0 TO LOWEST OF DISABLILTYNUM OR CYBERSENIORDUM (WARNING FOR WEB IF NOT WITHIN RANGE: Your answer cannot be more than the total number of director-level staff or of employees with a disability in cyber roles.)
2. DO NOT READ OUT: Don't know
3. DO NOT READ OUT: Prefer not to say

ASK IF HAVE NEURODIVERGENT PEOPLE IN CYBER ROLES (DISADVDUM CODE 4) AND MORE THAN ONE PERSON IN A CYBER ROLE (CYBERSIZEDUM≠1) AND ANSWERED HOW MANY IN SENIOR CYBER ROLES (CYBERSENIORDUM≥1)

Q20xe_NEUROSENIOR

IF ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM=1): Is this principal or director-level staff member a person with any neurodiverse conditions or learning disorders?

IF MORE THAN ONE PERSON IN A SENIOR CYBER ROLE (CYBERSENIORDUM≠1): How many of the principal or director-level staff members are people with any neurodiverse conditions or learning disorders?

ADD IF NECESSARY: We'd like an approximate number rather than a percentage.

SINGLE CODE

1. WRITE IN RANGE 0 TO LOWEST OF NEURONUM OR CYBERSENIORDUM (WARNING FOR WEB IF NOT WITHIN RANGE: Your answer cannot be more than the total number of director-level staff or of employees with neurodiverse conditions or learning disorders in cyber roles.)
2. DO NOT READ OUT: Don't know
3. DO NOT READ OUT: Prefer not to say

DUMMY VARIABLE NOT ASKED

Q20yb_FEMALESENIORDUM

Number of female staff in senior roles:

SINGLE CODE

- IF CYBERSIZEDUM=1 AND FEMALENUM≥0, TAKE ANSWER FROM FEMALENUM
- IF CYBERSIZEDUM≠1 AND FEMALESENIOR≥0, TAKE ANSWER FROM FEMALESENIOR

- ELSE MISSING

DUMMY VARIABLE NOT ASKED
Q20yc_BAMESENIORDUM
Number of staff from ethnic minorities in senior roles:

SINGLE CODE
- IF CYBERSIZEDUM=1 AND BAMENUM≥0, TAKE ANSWER FROM BAMENUM
- IF CYBERSIZEDUM≠1 AND BAMESENIOR≥0, TAKE ANSWER FROM BAMESENIOR
- ELSE MISSING

DUMMY VARIABLE NOT ASKED
Q20yd_DISABSENIORDUM
Number of disabled staff in senior roles:

SINGLE CODE
- IF CYBERSIZEDUM=1 AND DISABNUM≥0, TAKE ANSWER FROM DISABNUM
- IF CYBERSIZEDUM≠1 AND DISABSENIOR≥0, TAKE ANSWER FROM DISABSENIOR
- ELSE MISSING

DUMMY VARIABLE NOT ASKED
Q20y_NEUROSENIORDUM
Number of neurodivergent staff in senior roles:

SINGLE CODE
- IF CYBERSIZEDUM=1 AND NEURONUM≥0, TAKE ANSWER FROM NEURONUM
- IF CYBERSIZEDUM≠1 AND NEUROSENIOR≥0, TAKE ANSWER FROM NEUROSENIOR
- ELSE MISSING

Q21_DIVERSITYDUM DELETED IN 2020 QUESTIONNAIRE

Workforce qualifications (section deleted)

Q22_QUALS DELETED IN 2025 QUESTIONNAIRE

Q23_WHICHQUALS DELETED IN 2025 QUESTIONNAIRE

Q24_WHICHCERT DELETED IN 2021 QUESTIONNAIRE

Q25_SENIORITY DELETED IN 2020 QUESTIONNAIRE

Formal versus informal cyber security roles (section deleted)

Q26_FORMAL DELETED IN 2025 QUESTIONNAIRE

Q27_COVER DELETED IN 2021 QUESTIONNAIRE

Training and upskilling (section deleted)

Q_TRAININTROA DELETED IN 2023 QUESTIONNAIRE

Q_TRAININTROB DELETED IN 2023 QUESTIONNAIRE

Q_TRAINSCREENA DELETED IN 2023 QUESTIONNAIRE

Q_TRAINSCREENB DELETED IN 2023 QUESTIONNAIRE

Q35_VALUE DELETED POST-PILOT IN 2018 QUESTIONNAIRE

Q35a_NEEDSAWARE DELETED IN 2023 QUESTIONNAIRE

Q36_NEEDS DELETED IN 2023 QUESTIONNAIRE

Q_SOUGHT DELETED IN 2020 QUESTIONNAIRE

Q37a_TRAINED DELETED IN 2023 QUESTIONNAIRE

Q37b_FORMAT DELETED IN 2023 QUESTIONNAIRE

Q38_BARRIERS DELETED IN 2020 QUESTIONNAIRE

Q39_MODE DELETED IN 2020 QUESTIONNAIRE

Q40_TRAINER DELETED POST-PILOT IN 2018 QUESTIONNAIRE

Q41_TRAINERDUM DELETED POST-PILOT IN 2018 QUESTIONNAIRE

Q42_WORTH DELETED IN 2023 QUESTIONNAIRE

Staff turnover (cyber sector)

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND CYBER SECTOR (S_TYPE=3)
TURNOVERINTRO
I'd now like to ask about the staff turnover in cyber security job roles.

ASK IF CYBER SECTOR (S_TYPE=3)
Q47_LEFT
Since the start of 2023, have any employees in cyber security roles left your company or retired?

SINGLE CODE
1. Yes
2. No
3. DO NOT READ OUT: Don't know

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

ASK IF EMPLOYEES HAVE LEFT (LEFT CODE 1)
Q47c_LEFTA
Since the start of 2023, 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 ON SEPARATE SCREENS
a. Retirement
b. Dismissal
c. STATEMENT DELETED IN 2022 QUESTIONNAIRE
d. Redundancy
e. Of their own volition

SINGLE CODE
1. 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, "Did you say [ANSWER]?")
- IF MEDIUM/LARGE (SIZEA 49<CODE OR (SIZEB CODES 3 TO 5 OR DK): (SOFT CHECK IF >19)

2. 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
1. None
2. 1 to 2
3. 3 to 4
4. 5 to 9
5. 10 to 14
6. 15 to 19
7. 20 to 24
8. 25 to 29
9. More than 30
10. DO NOT READ OUT: Don't know

Q47e_REASON DELETED IN 2025 QUESTIONNAIRE

Recruitment (cyber sector)

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND CYBER SECTOR (S_TYPE=3)
RECRUITINTRO
I'd now like to ask about recruitment in cyber security job roles.

Q43_RECRUIT DELETED IN 2025 QUESTIONNAIRE

Q44_OTHRECRUIT DELETED IN 2025 QUESTIONNAIRE

ASK IF CYBER SECTOR (S_TYPE=3)
Q45_VACANCIES
Since the start of 2023, how many vacancies, if any, have you had in cyber security roles?
PROBE FOR BEST ESTIMATE BEFORE CODING DK

SINGLE CODE
1. WRITE IN RANGE 0 TO 99
   - IF MICRO (SIZEA CODE<10 OR SIZEB CODE 1): (SOFT CHECK IF >3, "Did you say [ANSWER]?")
   - 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)
2. DO NOT READ OUT: Don't know

ASK IF TRIED TO RECRUIT (VACANCIES>0 OR DK)
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

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

ASK IF HARD-TO-FILL VACANCIES (HARD>0 OR DK)

Q46b_HARDROLE

For this question, we would like you to look again at the UK Cyber Security Council's 16 cyber security specialisms online. You can Google "Cyber Career Framework, or I can give you the exact weblink.

ADD IF NECESSARY: https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

IF ONE HARD-TO-FILL VACANCY (HARD=1): Which **one** of these specialisms best describes this hard-to-fill role? You can give more than one answer if the role covered more than one specialism.
IF MORE THAN ONE HARD-TO-FILL HARD (HARD>1 OR DK): Which of these specialisms best describes these hard-to-fill roles? You can give more than one answer if the roles covered more than one specialism.
PROMPT TO CODE
PROBE FULLY (I.E. "ANY OTHER SPECIALISM?")
INTERVIEWER NOTE: IF JUST "ANALYST" OR "CONSULTANT", PROMPT WITH SPECIALIST ROLES BEFORE CODING "ANOTHER AREA".

MULTICODE

1. **Cryptography and Communications Security** – the designing, development, testing, implementation and operation of a system or product to provide cryptographic or secure communications
2. **Cyber Security Audit and Assurance** – the verification that systems and processes meet the specified security requirements and that processes to verify on-going compliance are in place
3. **Cyber Security Governance and Risk Management** – the monitoring of compliance with agreed cyber security policies and the assessment and management of relevant risks
4. **Cyber Security Management** – the management of cyber security resources, staff and policies at an enterprise level in line with business objectives and regulatory requirements
5. **Cyber Threat Intelligence** – the assessment, validation and reporting of information on current and potential cyber threats to maintain an organisation's situational awareness
6. **Data Protection and Privacy** – the management of the protection of data, enabling an organisation to meet its contractual, legal and regulatory requirements
7. **Digital Forensics** – the process of identifying and reconstructing the relevant sequence of events that have led to the currently observable state of a target IT system
8. **Identity and Access Management** – the management of policies, procedures and controls to ensure that only authorised individuals access information or computer-controlled resources
9. **Incident Response** – the preparation for, handling of and following up of cyber security incidents, to minimise the damage to an organisation and prevent recurrence
10. **Network Monitoring and Intrusion Detection** – the monitoring of network and system activity to identify unauthorised actions by users or potential intrusion by an attacker
11. **Secure Operations** – the management of an organisation's information systems operations in accordance with the agreed Security Policy
12. **Secure System Architecture and Design** – the designing of an IT system to meet its security requirements, balancing this with its functional requirements
13. **Secure System Development** – the development and updating of a system or product, in conformance with agreed security requirements and standards, throughout its lifecycle
14. **Security Testing** – the testing of a network, system, product or design, against the specified security requirements and/or for vulnerabilities (penetration testing)
15. **Vulnerability Management** – the management of the configuration of protected systems to

ensure that any vulnerabilities are understood and managed

16. **Another area** WRITE IN

SINGLE CODE

17. DO NOT READ OUT: Don't know

ASK IF HARD-TO-FILL VACANCIES (HARD>0 OR DK)

Q46b_HARDSENIOR

IF ONE HARD-TO-FILL VACANCY (HARD=1): What level of seniority was this hard-to-fill vacancy?
IF MORE THAN ONE HARD-TO-FILL VACANCY (HARD>1 OR DK): What levels of seniority were these hard-to-fill vacancies? You can give an answer for each vacancy.

PROMPT TO CODE

MULTICODE UP TO HARD (ERROR MESSAGE FOR WEB: "You said you had [HARD] hard-to-fill vacancy/vacancies in total.")

1. Apprentices
2. Entry-level staff or graduates
3. Experienced or senior staff, typically with around 3 to 5 years of experience
4. Principal-level staff, typically with around 6 to 9 years of experience
5. Director-level, typically with around 10 or more years of experience

SINGLE CODE

6. DO NOT READ OUT: Don't know

Q47_HARDREASON DELETED IN 2025 QUESTIONNAIRE

Q47a_DIVERSERECRUIT DELETED IN 2025 QUESTIONNAIRE

Q47AB_BARRIERSASK DELETED IN 2025 QUESTIONNAIRE

ASK IF TRIED TO RECRUIT (VACANCIES>0)

Q47e_DIVERSEACTION

Since the start of 2023, have you carried out any of the following to encourage applications from diverse groups?

READ OUT

RANDOMISE STATEMENT ORDER
ASK ON SEPARATE SCREENS IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB

a. Set diversity quotas for recruitment
b. Hired through non-degree routes
c. Worked with any non-profit organisations to find more diverse candidates
d. Hired through a government-backed scheme to promote diversity
e. Run talks or events in schools, colleges or universities
f. Attended networking events or career fairs specifically for diverse groups
g. Diversified our senior leadership team
h. Worked with recruitment agencies to find more diverse candidates

SINGLE CODE

1. Yes
2. No
3. DO NOT READ OUT: Not applicable to our business/have not filled vacancies
4. DO NOT READ OUT: Don't know

Q47b_INTERN DELETED IN 2025 QUESTIONNAIRE

Q47c_ENTRY DELETED IN 2025 QUESTIONNAIRE

Workforce expectations (both cyber sector and outside cyber sector)

ASK ALL
Q47f_FUTURE
Over the next 12 months, compared with the last 12 months, do you expect the number of people working in cyber security roles within your organisation to…?
READ OUT

SINGLE CODE, REVERSE SCALE
1. Increase
2. Stay about the same
3. Decrease
4. DO NOT READ OUT: Don't know

AI skills (cyber sector)

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND CYBER SECTOR (S_TYPE=3)
AITINTRO
These next questions are about AI skills. By AI skills, we mean the skills to apply AI concepts or algorithms in cyber security, such as machine learning, neural networks, and Supervised Learning algorithms.

SHOW IF ONLINE RESPONDENT (MODETYPE=WEB/ONLINE) AND CYBER SECTOR (S_TYPE=3)
AISCREEN
These next questions are about AI skills. By AI skills, we mean the skills to apply AI concepts or algorithms in cyber security, such as machine learning, neural networks, and Supervised Learning algorithms.

ASK IF CYBER SECTOR (S_TYPE=3)
Q47g_AIUSE
Currently, does anyone in a cyber security role in your business use AI skills in their day-to-day work?

ADD IF NECESSARY: By AI skills, we mean the skills to apply AI concepts or algorithms in cyber security, such as machine learning, neural networks, and Supervised Learning algorithms.

SINGLE CODE
1. Yes
2. No
3. DO NOT READ OUT: Don't know

ASK IF TRIED TO RECRUIT (VACANCIES>0)
Q47h_AIRECRUIT
Since the start of 2023, have you recruited anyone with AI skills into a cyber security role?

ADD IF NECESSARY: By AI skills, we mean the skills to apply AI concepts or algorithms in cyber security, such as machine learning, neural networks, and Supervised Learning algorithms.

SINGLE CODE
1. Yes
2. No
3. DO NOT READ OUT: Don't know

ASK IF CYBER SECTOR (S_TYPE=3)
Q47i_AITRAIN
Since the start of 2023, has anyone in a cyber security role in your business, including you, received training on AI concepts or algorithms?

SINGLE CODE
1. Yes
2. No
3. DO NOT READ OUT: Don't know

ASK IF CYBER SECTOR (S_TYPE=3)
Q47j_AIFUTURE
Over the next 12 months, compared with the last 12 months, do you expect the need for AI skills among people in cyber security roles in your business to…?

ADD IF NECESSARY: By AI skills, we mean the skills to apply AI concepts or algorithms in cyber security, such as machine learning, neural networks, and Supervised Learning algorithms.
READ OUT

SINGLE CODE, REVERSE SCALE
1. Increase
2. Stay about the same
3. Decrease
4. IF DO NOT CURRENTLY USE AI (AIUSE CODE 2): DO NOT READ OUT: We do not currently use AI, and do not expect to use AI
5. DO NOT READ OUT: Don't know

Export activity (cyber sector)

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND CYBER SECTOR (S_TYPE=3)
EXPORTINTRO
I'd now like to finish off with some broader questions about your cyber security business.

ASK IF CYBER SECTOR (S_TYPE=3)
Q14_EXPORTB
In your most recently completed financial year, approximately what percentage of your turnover **from your cyber security business** was attributable to exports?

ADD IF NECESSARY: By exports, we mean where products or services are purchased and used overseas by non-UK customers or clients.
PROMPT TO CODE

SINGLE CODE
1. 0%, i.e. none of it
2. 1% to 24%
3. 25% to 49%
4. 50% to 74%
5. 75% to 99%
6. 100%, i.e. all of it
7. DO NOT READ OUT: Have not started trading yet
8. DO NOT READ OUT: Don't know

ASK IF EXPORT (EXPORTB CODE 2-6)
Q15_REGION
In which of the following regions of the world are your non-UK customers based?
READ OUT

MULTICODE
1. The European Union
2. Wider Europe, outside the European Union (including Israel)
3. North America

4. Central or South America
5. The Gulf states, ADD IF NECESSARY: including Bahrain, Iraq, Kuwait, Oman, Qatar, Saudi Arabia, the United Arab Emirates and Yemen
6. Africa
7. Asia-Pacific, ADD IF NECESSARY: including East Asia, South Asia, Southeast Asia, Australia and New Zealand

SINGLE CODE

8. DO NOT READ OUT: Don't know

ASK IF DO NOT EXPORT (EXPORTB CODE 1 OR 7)

Q15b_NOEXPORT

Have you previously considered exporting your cyber security products or services to non-UK customers or clients?

SINGLE CODE

1. Yes
2. No
3. DO NOT READ OUT: Don't know

Sector networks and engagement (cyber sector)

ASK IF CYBER SECTOR (S_TYPE=3)

Q28c_ENGAGEMENT

In the region **of the UK** where you are headquartered, which of the following, if any, has your business collaborated or engaged with in the past 12 months, outside of day-to-day sales?

READ OUT

MULTICODE AND RANDOMISE CODES 1-5

1. A regional Cyber Security Cluster
2. A Local Enterprise Partnership or Regional Economic Development Agency
3. A regional Cyber Resilience Centre
4. A university or other higher education provider
5. Any Meetup events
6. Any other cyber security businesses
7. Any other public sector bodies
8. Any other organisations WRITE IN

SINGLE CODE

9. DO NOT READ OUT: None of these
10. DO NOT READ OUT: Don't know

Skills and knowledge of responsible individual or team (outside cyber sector)

Q28_RELATIVE DELETED IN 2025 QUESTIONNAIRE

ASK IF NOT CYBER SECTOR (S_TYPE≠3)

Q28a_RELATIVEX

How important would you say it is for all the employees in cyber security roles within your organisation to possess **high-level technical skills**?

This could include things like:

- security engineering or architecture
- penetration testing or vulnerability scanning
- using threat intelligence tools
- forensic analysis

- interpreting malicious code
- deploying automated cyber defences
- or using tools to monitor user activity

Please answer on a scale of 0 to 10, where 0 means not at all important and 10 means essential.

SINGLE CODE
WEB:
REVERSE SCALE

0. 0 – not at all important
1. 1
2. 2
3. 3
4. 4
5. 5
6. 6
7. 7
8. 8
9. 9
10. 10 – essential

CATI:

11. WRITE IN RANGE 0 TO 10

BOTH:

12. DO NOT READ OUT: Don't know

SCRIPT TO ROTATE ORDER OF TECHNICAL (KEPT WITH HIGHTECHNICAL) AND MANAGERIAL

ASK IF NOT CYBER SECTOR (S_TYPE≠3)
Q29_TECHNICAL
How confident, if at all, would you feel about you or any of the other individuals directly involved in cyber security within your organisation 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
ASK ON SEPARATE SCREENS IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB

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. **STATEMENT DELETED IN 2023 QUESTIONNAIRE**
k. **STATEMENT DELETED IN 2023 QUESTIONNAIRE**
l. **STATEMENT DELETED IN 2023 QUESTIONNAIRE**
m. **STATEMENT DELETED IN 2021 QUESTIONNAIRE**
n. **STATEMENT DELETED IN 2021 QUESTIONNAIRE**
o. **STATEMENT DELETED IN 2021 QUESTIONNAIRE**
p. ASK IF NOT OUTSOURCED (WHATOUTk NOT CODE 1): Setting up new user accounts and authentications securely

SINGLE CODE, REVERSE SCALE
1. Very confident
2. Fairly confident
3. Not very confident
4. Not at all confident
5. DO NOT READ OUT: Don't know
6. FOR STATEMENTS e AND g ONLY: DO NOT READ OUT: Not applicable – no devices belonging to organisation

ASK IF NOT CYBER SECTOR (S_TYPE≠3) AND HIGHER-LEVEL SKILLS MATTER (RELATIVEX>4) AND NOT ALL OUTSOURCED (ANY WHATHIGHER NOT CODE 1)

Q29_HIGHTECHNICAL

And how confident, if at all, would you feel about you or any of the other individuals directly involved in cyber security within your organisation being able to do each of the following **high-level technical** tasks in your work?

CATI: If these specific tasks are not relevant for your organisation, just say so and we'll move on.

WEB: If these specific tasks are not relevant for your organisation, please select Not applicable for each.

READ OUT
INTERVIEWER NOTE: IF CONFIDENCE LEVELS VARY ACROSS STAFF MEMBERS, THIS IS ABOUT THE MOST CONFIDENT STAFF MEMBER

RANDOMISE STATEMENT ORDER
ASK ON SEPARATE SCREENS IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB

a. ASK IF NOT OUTSOURCED (WHATHIGHERa NOT CODE 1): Designing secure networks, systems and application architectures
b. ASK IF NOT OUTSOURCED (WHATHIGHERb NOT CODE 1): Carrying out a penetration test
c. ASK IF NOT OUTSOURCED (WHATHIGHERc NOT CODE 1): Using cyber threat intelligence tools or platforms
d. ASK IF NOT OUTSOURCED (WHATHIGHERd NOT CODE 1): Carrying out a forensic analysis of a cyber security breach
e. ASK IF NOT OUTSOURCED (WHATHIGHERe NOT CODE 1): Interpreting malicious code
f. ASK IF NOT OUTSOURCED (WHATHIGHERf NOT CODE 1): Using tools to monitor user activity
g. ASK IF NOT OUTSOURCED (WHATHIGHERg NOT CODE 1): Carrying out vulnerability scans of the organisation's network and devices
i. ASK IF NOT OUTSOURCED (WHATHIGHERh NOT CODE 1): Deploying autonomous cyber defences

SINGLE CODE, REVERSE SCALE
1. Very confident
2. Fairly confident
3. Not very confident
4. Not at all confident
5. DO NOT READ OUT: Don't know

6. DO NOT READ OUT: Not applicable – we do not need to do these tasks in our organisation

ASK IF NOT CYBER SECTOR (S_TYPE≠3)

Q30_MANAGERIAL

How confident, if at all, would you feel about you or any of the other individuals directly involved in cyber security within your organisation 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
ASK ON SEPARATE SCREENS IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB

a. ASK HALF THE SAMPLE (HALF A): Communicating cyber security risks effectively to directors, trustees or senior management
b. **STATEMENT DELETED IN 2023 QUESTIONNAIRE**
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. **STATEMENT DELETED IN 2023 QUESTIONNAIRE**
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 QUESTIONNAIRE**
i. ASK HALF THE SAMPLE (HALF B): Developing cyber security policies
j. ASK HALF THE SAMPLE (HALF A): Developing a cyber security strategy, i.e. a document that underpins all your policies and processes
k. ASK HALF THE SAMPLE (HALF B) IF OUTSOURCE CYBER SECURITY (OUTSOURCE CODE 1): Assessing whether your external cyber security providers are offering value for money

SINGLE CODE, REVERSE SCALE

1. Very confident
2. Fairly confident
3. Not very confident
4. Not at all confident
5. DO NOT READ OUT: Don't know

Q31_KNOWLEDGE DELETED IN 2023 QUESTIONNAIRE

Skills and knowledge of wider staff (outside cyber sector)

SCRIPT TO BASE BUSINESS/CHARITY [directors/trustees] AND [staff/staff or volunteers] TEXT SUBSTITUTIONS ON S_TYPE (USE CHARITY TEXT IF S_TYPE=2, ELSE BUSINESS TEXT)

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI) AND NOT CYBER SECTOR (S_TYPE≠3)

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 (MODETYPE=WEB/ONLINE) AND NOT CYBER SECTOR (S_TYPE≠3)

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 (S_TYPE≠3)

Q32_DIRECTORS

How well, if at all, would you say your organisation's [directors/trustees] or senior managers [IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1-2):, including council members,] understand each of the following?

READ OUT

RANDOMISE STATEMENT ORDER
ASK ON SEPARATE SCREENS IF CATI
ASK AS A COLLAPSIBLE GRID IF WEB

a. The cyber security risks facing your organisation
b. **STATEMENT DELETED IN 2023 QUESTIONNAIRE**
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 QUESTIONNAIRE**
f. **STATEMENT DELETED POST-PILOT IN 2018 QUESTIONNAIRE**
g. **STATEMENT DELETED POST-PILOT IN 2018 QUESTIONNAIRE**
h. The staffing needs of cyber security within your organisation

SINGLE CODE, REVERSE SCALE

1. Very well
2. Fairly well
3. Not very well
4. Not at all well
5. DO NOT READ OUT: Don't know

Q33_DIRECTDUM DELETED IN 2020 QUESTIONNAIRE

ASK IF NOT CYBER SECTOR (S_TYPE CODE≠3)

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=1-2): or council members] as a whole being able to do each of the following?

READ OUT

RANDOMISE STATEMENT ORDER
ASK ON SEPARATE SCREENS IF CATI OR WEB (REFLECTING EXTRA RESPONSE CODE FOR STATEMENT d)

a. STATEMENT DELETED POST-PILOT IN 2018 QUESTIONNAIRE
b. ASK HALF THE SAMPLE IF PRIVATE SECTOR (HALF A AND S_TYPE=1) OR FULL SAMPLE IF PUBLIC SECTOR OR CHARITY (S_TYPE=2 OR 4): Store or transfer personal data securely, using encryption where appropriate
c. STATEMENT DELETED IN 2025 QUESTIONNAIRE
d. ASK HALF THE SAMPLE IF PRIVATE SECTOR (HALF A AND S_TYPE=1) OR FULL SAMPLE IF PUBLIC SECTOR OR CHARITY (S_TYPE=2 OR 4): Detect malware on the organisation's devices
e. ASK HALF THE SAMPLE IF PRIVATE SECTOR (HALF B AND S_TYPE=1) OR FULL SAMPLE IF PUBLIC SECTOR OR CHARITY (S_TYPE=2 OR 4): Identify fraudulent emails or fraudulent websites
f. ASK HALF THE SAMPLE IF PRIVATE SECTOR (HALF B AND S_TYPE=1) OR FULL SAMPLE IF PUBLIC SECTOR OR CHARITY (S_TYPE=2 OR 4): Work collaboratively with those directly responsible for dealing with cyber security breaches

SINGLE CODE, REVERSE SCALE

1. Very confident
2. Fairly confident

3. Not very confident
4. Not at all confident
5. DO NOT READ OUT: Don't know
6. FOR STATEMENT d ONLY: DO NOT READ OUT: Not applicable – no devices belonging to organisation

Recontact

ASK IF CYBER SECTOR (S_TYPE=3)

Q48b_PANEL

Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, and we are going to contact the UK cyber sector again in around 12 months. Would you be happy for Ipsos to maintain your individual contact details for 12 months, to save us from having to contact any switchboard next time? Participation in any later years would still be voluntary and you can opt out at any point.

SINGLE CODE

1. Yes
2. No

ASK ALL

Q48_RECON

Would you be willing to be invited to a more in-depth interview with Ipsos within the next 6 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.

ADD IF NECESSARY: Everyone taking part in these further interviews would be offered £70, either as a bank transfer, or as a donation to the charity of their choice.

SINGLE CODE

1. Yes
2. No

Q48a_DCMSRECON DELETED IN 2025 QUESTIONNAIRE

Q49a_WEBFOLLOW DELETED IN 2025 QUESTIONNAIRE

ASK IF WANT PANEL RECONTACT (PANEL CODE 1) OR QUALITATIVE RECONTACT (RECON CODE 1)

Q51_PANELCONTACT

Can we confirm some contact details?

PROBE FULLY

MULTICODE

1. Name WRITE IN
2. Job title WRITE IN
3. Email WRITE IN EMAIL IN VALIDATED FORMAT
4. Phone WRITE IN TELEPHONE NUMBER IN VALIDATED FORMAT
5. Another person to ask for if you are away WRITE IN

SINGLE CODE

6. DO NOT READ OUT: Prefer not to say

ASK IF WANT HELP CARD (HELPCARD CODE 1) AND NOT QUALITATIVE RECONTACT (RECON CODE 2)

Q50_EMAIL

At the start of this interview, you said you would like us to email you a government help card, with links to the latest official cyber security guidance for organisations. Can we please take an email address for this?

SINGLE CODE

1. WRITE IN EMAIL IN VALIDATED FORMAT
2. DO NOT READ OUT: Prefer not to say

SEND FOLLOW-UP EMAIL IF WANT HELP CARD AND GIVE EMAIL (EMAIL CODE 1)

GDPR privacy policy

READ OUT IF TELEPHONE RESPONDENT (MODETYPE=CATI)

GDPRINTRO

Thank you for taking the time to participate. You can access the privacy policy on the gov.uk website at: https://www.gov.uk/government/publications/understanding-the-uk-cyber-security-sector-and-labour-market. 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 (MODETYPE=WEB/ONLINE)

GDPRSCREEN

Thank you for taking the time to participate. You can access the privacy policy on the gov.uk website at: https://www.gov.uk/government/publications/understanding-the-uk-cyber-security-sector-and-labour-market. 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 Science, Innovation, & Technology

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.

Ipsos (market research) Ltd, Registered in England and Wales No 948470

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

Government guidance for organisations on cyber security

Department for Science, Innovation, & Technology

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 – https://www.ncsc.gov.uk/collection/board-toolkit

The NCSC's Board Toolkit helps boards to ensure that cyber resilience and risk management are embedded throughout an organisation, including its people, systems, processes and technologies.

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

Ipsos (market research) Ltd, Registered in England and Wales No 948470

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

Appendix C: Topic guide for cyber security businesses

Using this guide

The topic guide uses the following conventions: **bold** for questions that should be covered in every interview, bulleted probes for follow-up questions, and *italics* for moderator instructions.

NB When using the guide, the researcher will ask questions and prompts and will use probes to guide where necessary. Probes are asked where the participant does not bring something up spontaneously in response to a question (and the probe is relevant for their particular business). Not all questions or probes will necessarily be used during the interview.

Before each interview: The interviewer will undertake some preparation work including background reading on the participant's organisation and role, as well as the UK Cyber Security Council's Cyber Career Framework (www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/) and Professional Standards (www.ukcybersecuritycouncil.org.uk/professional-standards-registration/).

Introduction	2 - 3 mins
▪ **Introduce yourself and Ipsos**. ▪ **Explain research RECONTACT SAMPLE ONLY:** Recently you took part in a survey with us on behalf of the Department for Science, Innovation and Technology (DSIT). At the time, you said you would be willing to be invited to take part in an in-depth interview for this study. The interview will give you the opportunity to give more detailed feedback, in your own words, about the areas of growth, cyber skills, and recruitment needs within your organisation as well as in the UK cyber security sector more generally. The format is different to a survey and will be more of a conversation. These in-depth interviews will provide the government with a more detailed understanding of these issues. Your feedback helps the government gain a better overview on how organisations like yours may benefit from further guidance, training or support. ▪ **Explain research LEADS / DESK RESEARCH SAMPLE ONLY:** [Name] at [Organisation] recommended you as someone we should speak to. Ipsos and Perspective Economics are carrying out important research on the UK cyber security sector on behalf of the Department for Science, Innovation and Technology (DSIT). As part of this research, we would like to invite you to an interview. In this interview, we will be asking you for feedback about the areas of growth, cyber skills, and recruitment needs within your organisation as well as in the UK cyber security sector more generally. These in-depth interviews will help the government gain a better understanding of how organisations such as your own may benefit from further guidance, training or support. ▪ **The interview:** The discussion will be informal. There are no right or wrong answers. ▪ **Explain confidentiality**: The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no	

identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties. ▪ **Explain payment for participation**. You will receive £70 [IF RECONTACT SAMPLE]/£100 [IF NOT RECONTACT SAMPLE] as either a bank transfer or charity donation as a thank you for your time. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.) ▪ **Explain voluntary participation**: If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary. ▪ **Length of the interview**: This discussion will last a maximum of 60 minutes. ▪ **Questions**: Do you have any questions before we begin? ▪ **Consent to audio record**: I would like to record our discussion as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely and deleted 12 months after the interview takes place. *MODERATOR TO TURN ON RECORDING* <u>GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON)</u> Ipsos's legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview and before data is anonymised at the end of November 2024. Can I check that you are happy to proceed?	
1. Business background and context	**2 min**
Firstly, please could you briefly describe your role? • How long have you been working in this organisation / business? • What are your responsibilities? **Please could you briefly tell me about your organisation / business?**	
2. Trends in customer demand	**12 mins**
Can you please describe the current state of the cyber security sector? What, if any, are the biggest challenges you see in cyber security today? **In your opinion, what are the most significant market trends currently shaping the cyber security sector?** • Why are these the most significant trends? **Can you please tell me about your customers? Which, if any, cyber security products and services are your customers most interested in, and why?** *PROBE ON: sector, location, size* • What, if anything, has changed since last year?	

Which particular technologies are driving demand in the cyber security market currently, compared to last year? • Why do you think these technologies are becoming more popular? • How, if at all, are these technologies being integrated into your cyber security offer? • What challenges, if any, do you face when implementing these technologies? Have these challenges changed since last year? **What factors influence your clients' decisions to purchase or not purchase cybers security products and services? What, if any, cyber security products or services are customers hesitant to adopt?** • Why is this? • Has there been any shift in hesitation around these products since last year? **What, if any, are the biggest commercial opportunities you see in cyber security today?** • Why are these the biggest commercial opportunities? • How, if at all, have these commercial opportunities changes from last year? **Which cyber security products and services are your clients most interested in, and why? How, if at all, has this changed over the last 12 months?** *PROBE VARIATIONS BY: customer type, domain or technology* • Why is this? IF NOT ALREADY RAISED, ASK: **Do you provide cyber security solutions for AI models and systems?** • *IF YES:* How, if at all, has demand for these solutions developed compared to last year? • **Does your organisation use any AI models or systems in its overall business?**	
3. Growth areas, emerging opportunities in cyber security – PRIORITY SECTION	**12 mins**
How do you see the cyber sector evolving in the next 5 years? What factors are going to shape this? How, if at all, do you foresee your organisation or sector adapting to this evolution? • Why do you see it evolving in this way? **What, if any, are the growth areas you see in cyber security in the next 5 years? Why?** **What are your plans for growth?** *PROBE ON: investment, availability of skills* • Do you expect your business to grow, stay the same or decline in the next 5 years? Why is this? • What, if any, factors might influence this?	

What role, if any, will AI and machine learning play in the future of cyber security? • Why do you see it playing this role? **How, if at all, has AI and automation impacted your customers' cyber security needs and priorities? What, if any, impact do you think this will have on in the future?** • Why is this? **How, if at all, do you expect demand for cyber security solutions for AI models and systems to change?** • Why is this? **How, if at all, do you see emerging technologies influencing customer demand for cyber security products and services? (for example, quantum)** • Why is this? • Which, if any, specific emerging technologies are gaining traction among your customers? Why is this? • How, if at all, do you plan to adapt your offer to incorporate these emerging technologies? • What, if any, are the potential risks and benefits associated with these emerging technologies? Why is this? **How can cyber security companies like yours identify and enter untapped markets? Or regions? What sort of support, if any, would be beneficial?** • Why is this? **What are the factors which will help the growth of the cyber security sector? And what are the factors that will hinder growth?** • Why is this? **What difference could the availability of investment make?** • Why is this? **What role, if any, does government have?** • Why is this?	
4. Access to and demand for talent	**7 mins**
Please describe the cyber team / staff in your organisation. How, if at all, has this changed in the last 12 months? **What, if any, skills are missing in your cyber team?** *PROBE ON: technical skills, incident response, complementary and governance skills* • Why are they missing?	

Thinking about AI cyber skills, in what ways, if any, does your business use AI skills (for example, machine learning techniques) in cyber security practices and processes (for example, to detect or mitigate adversarial attacks) • Are you looking into adopting further AI skills in the future? • *IF SO*, what specific areas are you focusing on? Why • *IF NOT*, why not? *PRODUCT FIRMS ONLY*: **Does anyone in a cyber security role in your business use AI concepts or develop AI algorithms as part of their day-to-day work?** *IF YES, ASK:* • How far, if at all, do cyber staff have specific expertise in the cyber security of AI models and systems themselves i.e. skills to protect AI models or systems? • How confident are you that your business has the skills to secure AI models and systems? • What, if any, training has been provided? **How many staff, if any, have you recruited in the last 12 months? How much of a challenge is it to recruit people for cyber roles in your organisations? Which roles, if any, are the most challenging to recruit for and why?** **What recruitment methods, if any, have been most successful for you in the past year? How, if at all, might your recruitment methods change in the future?** • Why is that? **How, if at all, do you assess whether job applicants for cyber security roles are proficient?** • What do you especially look for? Why is this? • What would put you off hiring a candidate? Why is this? **How long do cyber security staff generally stay in your organisation? Which cyber security staff do you think have been or are most likely to leave your organisation?** • Why is this? **What, if any, factors do you think contribute to employees staying longer or shorter in cyber roles? What, if any, strategies have you put in place to retain your cyber staff?** • Why is this?	
5. Outsourcing - ASK MANAGED SERVICES FIRMS ONLY	**5 mins**
What, if any, outsourcing services do you offer? • Why do you offer these? **How do customers choose outsourcing providers for cyber security in your experience?** • How knowledgeable are customers in choosing providers?	

• And different cyber security solutions? **How, if at all, might customer outsourcing needs change in the future?** • Why is this? **How has your experience with the UK cyber security ecosystem, particularly the role of managed service providers, evolved in recent years?** *ADD IF NECESSARY:* An outsourced provider refers to any third-party vendor that handles specific cyber security fundings, whereas an MSP refers to a third-party company that remotely manages a customer's IT infrastructure or end-user systems on a more proactive basis. • Why do you think these changes have occurred? • How, if at all have these changes impacted your outsourcing / business decisions? • How do you see the role of MSPs evolving in the future?	
6. Diversity of labour market	**4 mins**
What do you think of when we talk about diversity in the cyber sector? What does this refer to? How diverse is the cyber sector? • Why is this? **How, if at all, has this changed / evolved in the last two years?** • What specific changes, if any, have you seen? **What, if any, recruitment strategies are in place to recruit a diverse cyber workforce for your organisation?** • Why are these in place? **What challenges, if any, do you face when trying to improve diversity in your cyber security workforce?** • Why is that? • Which, if any, of these challenges are specific to the cyber security sector, the broader tech sector, or common to all employers? Why is this? • Have you tried to address these challenges, and what has been the result?	
7. Entry-level pathways and expectations	**5 mins**
What is your approach to entry-level roles? How about work placements or apprenticeships? *PROBE ON: how candidates are sourced (and which approaches work best), minimum requirements, diversity of entry level recruits, retention of entry level recruits* • Why have you taken this approach? • How, if at all, has this changed in the past couple of years? Why is this? **What would encourage your organisation to offer more / start offering entry-level roles in cyber security?**	

• Why is this? **To what extent, if any, are you engaging with educational institutions? What engagement would be helpful for entry-level roles?** • Why is this? **What steps, if any, should the cyber security industry be taking in supporting entry-level pathways? What is the role, if any, of educational institutions in entry-level roles in cyber security?** **How, if at all, are entry-level roles in cyber security changing in the current landscape?** • Why is this? • What new trends or challenges are emerging for entry-level positions? • How, if at all, are organisations adapting to these changes?	
8. Cyber Career Framework and UK Cyber Security Council's professional standards	**5 mins**
Participants will have been sent a link to the UK Cyber Security Council 16 specialisms and Cyber Career Framework 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: www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/ **What, if anything, had you seen / heard of the 16 cyber security specialisms and the UK Cyber Security Council's Cyber Career Framework before taking part in this research?** **How, if at all, helpful is the Cyber Career Framework?** • How, if at all, is it being used by your cyber team / business? Why is this? • How likely, if at all, would you be to use this resource in your organisation in the future? Why / Why not? • What, if anything, could be added or improved to make it more suitable for your needs? Why have you suggested this? **What impact, if any, could the framework have on developing a shared understanding of cyber roles?** • Why is this? • How, if at all, could it have more impact? Why is this? **What, if anything, do you know about the UK Cyber Security Council's Professional Standards for each of the 16 specialisms?** *IF NECESSARY, EXPLAIN: The UK Cyber Security Council is developing professional standards for each specialism at three levels – associate, principal and chartered.* • How, if at all, likely would organisations / your organisation be to encourage employees to achieve these professional standards? Why / why not? • Does this differ by experience levels? Why is this?	

• What, if any, are the potential benefits versus the costs? Why is this?	
9. Future skills and training needs – PRIORITY SECTION	**7 mins**
Looking ahead, what cyber skills will be most important in the next 2-5 years? • Why is this? **How are the skills needs of your organisation likely to change? How, if at all, are you preparing for future changes in skills needs?** • Why is this? **What impact, if any, is AI likely to have on cyber skills and careers? How would you describe the skills required to ensure the cyber security of AI technologies?** *PROBE ON: entry-level roles/apprentices, career pathways, cyber specialisms / generalist roles* **What sort of training would be most beneficial in the future? What needs to happen to ensure sufficient training is available? Specifically on AI, what challenges are there in providing training?** **How can the industry overall ensure that the UK has the cyber security workforce it needs in the future? And what, if any, is the role of government?** • Why is this?	
Wrap up	**2 mins**
What is the key thing you would like to feed back to the Department for Science, Innovation and Technology about what we have discussed today? **Is there anything else you'd like to mention that we haven't had a chance to discuss?** **Thank you for your valuable contribution to this important research. Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, which will be taking place again next year. Would you be happy for us to recontact you to take part in this research again? If we were not talking to you, which of your colleagues would we reach out to?** **INCENTIVE**: Thank participant and remind them of confidentiality. Explain that they can get in touch if they have any further comments or questions about the research. Remind them of the £70 [IF RECONTACT SAMPLE]/£100 [IF NOT RECONTACT SAMPLE] as either a bank transfer or charity donation thank you from Ipsos, as an appreciation for their time and contribution to the research. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)	

Appendix D: Topic guide for cyber leads at non-cyber security-related businesses

Using this guide

The topic guide uses the following conventions: **bold** for questions that should be covered in every interview, bulleted probes for follow-up questions, and *italics* for moderator instructions.

NB When using the guide, the researcher will ask questions and prompts and will use probes to guide where necessary. Probes are asked where the participant does not bring something up spontaneously in response to a question (and the probe is relevant for their particular business). Not all questions or probes will necessarily be used during the interview.

Before each interview: The interviewer will undertake some preparation work including background reading on the participant's organisation and role, as well as the UK Cyber Security Council's Cyber Career Framework (www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/) and Professional Standards (www.ukcybersecuritycouncil.org.uk/professional-standards-registration/).

Introduction	2 - 3 mins
▪ **Introduce yourself and Ipsos**. ▪ **Explain research RECONTACT SAMPLE ONLY:** Recently you took part in a survey with us on behalf of the Department for Science, Innovation and Technology (DSIT). At the time, you said you would be willing to be invited to take part in an in-depth interview for this study. The interview will give you the opportunity to give more detailed feedback, in your own words, about the areas of growth, cyber skills, and recruitment needs within your organisation as well as in the UK cyber security sector more generally. The format is different to a survey and will be more of a conversation. These in-depth interviews will provide the government with a more detailed understanding of these issues. Your feedback helps the government gain a better overview on how organisations like yours may benefit from further guidance, training or support. ▪ **Explain research LEADS / DESK RESEARCH SAMPLE ONLY**: [Name] at [Organisation] recommended you as someone we should speak to. Ipsos and Perspective Economics are carrying out important research on the UK cyber security sector on behalf of the Department for Science, Innovation and Technology (DSIT). As part of this research, we would like to invite you to an interview. ▪ In this interview, we will be asking you for feedback about the areas of skills, and recruitment needs within your organisation as well as in the UK cyber security sector more generally. These in-depth interviews will help the government gain a better understanding of how organisations such as your own may benefit from further guidance, training or support.	

▪ **The interview:** The discussion will be informal. There are no right or wrong answers. ▪ **Explain confidentiality**: The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties. ▪ **Explain payment for participation**. You will receive £70 [IF RECONTACT SAMPLE]/£100 [IF NOT RECONTACT SAMPLE] as either a bank transfer or charity donation as a thank you for your time. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.) ▪ **Explain voluntary participation**: If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary. ▪ **Length of the interview**: This discussion will last a maximum of 60 minutes. ▪ **Questions**: Do you have any questions before we begin? ▪ **Consent to audio record**: I would like to record our discussion as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely and deleted 12 months after the interview takes place. *MODERATOR TO TURN ON RECORDING* <u>GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON)</u> Ipsos's legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview and before data is anonymised at the end of November 2024. Can I check that you are happy to proceed?	
1. Business background and context	**3 mins**
Firstly, please could you briefly describe your role? • How long have you been working in this organisation / business? • What are your responsibilities? **Please could you briefly tell me about your organisation / business?** • How long has the organisation / business been operating? • What does the organisation / business do? • How would you describe the size and structure of the organisation / business? **What, if any, are the biggest challenges your business/organisation faces in terms of cyber security?**	
2. Access to and demand for talent	**15 mins**
Please describe the cyber team / staff in your organisation. How, if at all, has this changed in the last 12 months? **What, if any, skills are missing in your cyber team?**	

PROBE ON: technical skills, incident response, complementary and governance skills

- Why are they missing?

How many staff, if any, have you recruited in the last 12 months? How, if at all, has this changed compared to previous years and why?

- Why have you recruited these staff?

How much of a challenge is it to recruit people for cyber roles in your organisations? Which roles, if any, are the most challenging to recruit for and why?

- Why is it a challenge?

To what extent, if any, is the cost of recruitment an issue?

- Why / why is it not an issue?

IF THEY HAVE RECENTLY HAD VACANCIES FOR CYBER ROLES THAT WERE HARD TO FILL:

You mentioned [*IN THE SURVEY IF APPROPRIATE*] that some roles were hard to fill.

What roles were hard to fill?

- Could you tell me what happened?
- Have these vacancies now been filled?

What recruitment methods, if any, have been most successful for you in the past year?

- Why were they successful?

How, if at all, might your recruitment methods change in the future?

- Why is that?

How, if at all, do you assess whether job applicants for cyber security roles are proficient?

- What do you especially look for? Why is this?
- What would put you off hiring a candidate? Why is this?

How long do cyber security staff generally stay in your organisation?

- How, if at all, does this compare to other roles?

Which cyber security staff do you think have been or are most likely to leave your organisation?

- Why is this?

What, if any, factors do you think contribute to employees staying longer or shorter in cyber security roles?

- Why is this?

What, if any, strategies have you put in place to retain your cyber staff? • Why is this?	
3. AI cyber skills	**5 mins**
Thinking about AI cyber skills, in what ways, if any, does your business use AI skills (for example, machine learning techniques) in cyber security practices and processes (for example, to detect or mitigate adversarial attacks) • Are you looking into adopting further AI skills in the future? • *IF SO*, what specific areas are you focusing on? Why • *IF NOT*, why not? **Does your organisation use any AI models or systems in its overall business operations?** • Are there any AI models or systems you have considered adopting? Why is this? • How far, if at all, do cyber staff have specific expertise in the cyber security of AI models and systems themselves i.e. skills to protect AI models or systems? • How confident are you that your business has the skills to secure AI models and systems? • What, if any, training has been provided? **How does your business approach purchasing AI-related cyber security solutions?** • What, if any, factors do you consider when deciding to invest in such solutions? • How, if at all, do you distinguish what is value for money versus what is not? **What challenges, if any, do you face in evaluating the cost-efficiency of AI cyber security products?**	
4. Entry-level pathways and expectations	**7 mins**
I would like us to think about entry-level roles in cyber security. What, if any, experience should people thinking about an entry-level role have? • Why is this? **What is your approach to entry-level roles? And work placements? And apprenticeships?** *PROBE ON: how candidates are sourced (and which approaches work best), minimum requirements, diversity of entry level recruits, retention of entry level recruits* • Why have you taken this approach? • How, if at all, has this changed in the past couple of years? Why is this? **What would encourage your organisation to offer more / start offering entry-level roles in cyber security?** • Why is this?	

To what extent, if any, are you engaging with educational institutions? What engagement would be helpful for entry-level roles? • Why is this? **What steps, if any, should the cyber security industry be taking in supporting entry-level pathways?** • Why is this? • What should educational institutions be doing? Why is this? • What, if any, is the role of government? Why is this? **What is the role, if any, of educational institutions in entry-level roles in cyber security? What should their role be?** • Why is this? **How, if at all, are entry-level roles in cyber security changing in the current landscape?** • Why is this? • What new trends or challenges are emerging for entry-level positions? • How, if at all, are organisations adapting to these changes?	
5. Cyber Career Framework and UK Cyber Security Council's professional standards	**5 mins**
Participants will have been sent a link to the UK Cyber Security Council 16 specialisms and Cyber Career Framework 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: www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/ **What, if anything, had you seen / heard of the 16 cyber security specialisms and the UK Cyber Security Council's Cyber Career Framework before taking part in this research?** **How, if at all, helpful is the Cyber Career Framework?** • How, if at all, is it being used by your cyber team / business? Why is this? • How likely, if at all, would you be to use this resource in your organisation in the future? Why / Why not? • What, if anything, could be added or improved to make it more suitable for your needs? Why have you suggested this? **What impact, if any, could the framework have on developing a shared understanding of cyber roles?** • Why is this? • How, if at all, could it have more impact? Why is this? **What, if anything, do you know about the UK Cyber Security Council's Professional Standards for each of the 16 specialisms?** *IF NECESSARY, EXPLAIN: The UK Cyber Security Council is developing professional standards for each specialism at three levels – associate, principal and chartered.*	

• How, if at all, likely would organisations / your organisation be to encourage employees to achieve these professional standards? Why / why not? • Does this differ by experience levels? Why is this? • What, if any, are the potential benefits versus the costs? Why is this?	
6. Outsourcing	**10 mins**
Which, if any, aspects of your cyber security do you outsource? *IF RECONTACT SAMPLE, PROBE ON SURVEY RESPONSES* *IF OUTSOURCE:* **What are the reasons for outsourcing these functions?** • Who was involved in this decision? **Which external providers do you use? Where are they based?** *PROBE FOR: UK vs non-UK* • Have you changed providers in the past 12 months, and if so, why? **How are providers chosen?** • Why is this? • How confident are you in choosing providers? Why is this? • How easy or difficult is it to understand different cyber solutions? Why is this? • Has this process becoming easier or harder in the current market, compared to previous years? Why is this? **What, if anything have you learned about good practices in outsourcing cyber security?** • Have you made any changes based on these learnings? Why / why not? **How did you / can you assess if your external providers have the necessary skills?** • How do you know if external providers are doing a good job? • Have your assessment criteria changed over time? Why / why not? **What difference, if any, does it make if a provider is not based in the UK?** *PROBE ON: pros and cons, confidence in choosing and assessing performance* • Has your perspective on this changed at all recently compared to previous years? Why is this? **What, if any, are your priorities for this year regarding outsourcing?** • Why is that? *ASK ALL:* **What are the advantages and disadvantages of outsourcing cyber security?** • Why are these advantages and disadvantages? • Have these changed recently compared to previous years?	

ASK ALL: **Do you plan to bring more cyber security functions in-house, stay with your current outsourcing model, or increase outsourcing in the next couple of years? How about in the next five years?** • Why is that? *ASK ALL:* **How has your experience with the UK cyber security ecosystem, particularly the role of managed service providers, evolved in recent years?** *ADD IF NECESSARY:* An outsourced provider refers to any third-party vendor that handles specific cyber security fundings, whereas an MSP refers to a third-party company that remotely manages a customer's IT infrastructure or end-user systems on a more proactive basis. • Why do you think these changes have occurred? • How, if at all have these changes impacted your outsourcing / business decisions? • How do you see the role of MSPs evolving in the future?	
7. Diversity of labour market	**5 mins**
What do you think of when we talk about diversity in the cyber sector? What does this refer to? How diverse is the cyber sector? • Why is this? **What kind of diversity do you think is lacking?** • Why is this? **How, if at all, has this changed / evolved in the last two years?** • What specific changes, if any, have you seen? **What, if any, recruitment strategies are in place to recruit a diverse cyber workforce for your organisation?** • Why are these in place? **What, if any, strategies would you consider in the future to diversify the cyber workforce in your organisation?** • Why is this? **What challenges, if any, do you face when trying to improve diversity in your cyber security workforce?** • Why is that? • Which, if any, of these challenges are specific to the cyber security sector, the broader tech sector, or common to all employers? Why is this? • Have you tried to address these challenges, and what has been the result?	
8. Future skills and training needs	**7 mins**

How, if at all, do you see the cyber sector evolving in the next 5 years? What factors are going to shape this? How, if at all, do you foresee your organisation or sector adapting to this evolution? **Looking ahead, what cyber skills will be most important in the next 2-5 years? What new skills or roles do you think will become more important? What changes have you seen already?** • Why is this? **How are the skills needs of your organisation likely to change? What, if any, concerns do you have? How, if at all, are you preparing for future changes in skills needs?** • Why is this? **What impact, if any, is AI likely to have on cyber skills and careers?** • Why is this? **How would you describe the skills required to ensure the cyber security of AI technologies?** *PROBE ON: entry-level roles/apprentices, career pathways, cyber specialisms / generalist roles* • How, if at all, do these differ from cyber security skills more generally? Why is this? **What are your current training needs and how are these likely to change in the future? What sort of training would be most beneficial in the future? How confident do you feel that this sort of training will be available?** • Why is this? **What needs to happen to ensure sufficient training is available? Specifically on AI, what challenges are there in providing training?** • Why is this? **How can the industry overall ensure that the UK has the cyber security workforce it needs in the future?** Why is this? **And what, if any, is the role of government?** • Why is this?	
Wrap up	**2 mins**
What is the key thing you would like to feed back to the Department for Science, Innovation and Technology about what we have discussed today? **Is there anything else you'd like to mention that we haven't had a chance to discuss?**	

Thank you for your valuable contribution to this important research. Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, which will be taking place again next year. Would you be happy for us to recontact you to take part in this research again? If we were not talking to you, which of your colleagues would we reach out to? **INCENTIVE**: Thank participant and remind them of confidentiality. Explain that they can get in touch if they have any further comments or questions about the research. Remind them of the £70 [IF RECONTACT SAMPLE]/£100 [IF NOT RECONTACT SAMPLE] as either a bank transfer or charity donation thank you from Ipsos, as an appreciation for their time and contribution to the research. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)	

Appendix E: Topic guide for recruitment agents

Using this guide

The topic guide uses the following conventions: **bold** for questions that should be covered in every interview, bulleted probes for follow-up questions, and *italics* for moderator instructions.

NB When using the guide, the researcher will ask questions and prompts and will use probes to guide where necessary. Probes are asked where the participant does not bring something up spontaneously in response to a question (and the probe is relevant for their particular business). Not all questions or probes will necessarily be used during the interview.

Before each interview: The interviewer will undertake some preparation work including background reading on the participant's organisation and role, as well as the UK Cyber Security Council's Cyber Career Framework (www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/) and Professional Standards (www.ukcybersecuritycouncil.org.uk/professional-standards-registration/).

Introduction	2 - 3 mins
▪ **Introduce yourself and Ipsos**. ▪ **Explain research**: Ipsos carries out an annual study on the cyber security labour market and sector on behalf of the Department for Science, Innovation and Technology (DSIT). This multi-year study has directly informed the government's 2022 to 2025 National Cyber Strategy. You might remember this study from previous years or even have taken part in the research before. As part of the study, we interview recruitment agents like you. This feedback provides us with invaluable information about cyber security skills and recruitment in the UK. ▪ **The interview:** The discussion will be informal. There are no right or wrong answers. ▪ **Explain confidentiality**: The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties. ▪ **Explain payment for participation**. You will receive £100 as either a bank transfer or charity donation as a thank you for your time. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.) ▪ **Explain voluntary participation**: If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary. ▪ **Length of the interview**: This discussion will last a maximum of 60 minutes. ▪ **Questions**: Do you have any questions before we begin? ▪ **Consent to audio record**: I would like to record our discussion as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely and deleted 12 months after the interview takes place.	

MODERATOR TO TURN ON RECORDING <u>GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON)</u> Ipsos's legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview and before data is anonymised at the end of November 2024. Can I check that you are happy to proceed?	
1. Business background and context	**3 mins**
Firstly, please could you briefly describe your role? • How long have you been working in this agency? • What is your experience of cyber security? **Please could you briefly tell me about your agency?** • How long has it been operating and how would you describe its size and structure? • What areas of recruitment does it specialise in?	
2. Trends in customer demand	**3 mins**
Can you please describe the current state of the cyber security sector? • Why have you described it in this way? **What, if any, are the biggest challenges you see in cyber security today?** • Why are these the biggest challenges? **In your opinion, what are the most significant market trends currently shaping the cyber security sector?** • Why are these the most significant trends?	
3. Labour market health and trends	**20 mins**
What are your clients' biggest needs presently, when recruiting for cyber roles? *PROBE ON: Skills, roles, specialisms* • Why are these their biggest needs? **How, if at all, have these needs evolved in the last year? What requirements have become more important?** • Why have they evolved / become more important? **How, if at all, do client demands vary according to location?** • How, if at all, important is the location to clients?	

• How, if at all, has this changed over the past year? • How, if at all, are demands for applicants, as well as layoffs regionally affecting recruitment conversations? **How, if at all, has the quality and type of candidates in the cyber recruitment pool changed in the past year?** • Why has it changed like this? **How, if at all, has the quantity of applicants changed over the past year?** • Why has it changed like this? **What would you say are the biggest gaps in the recruitment pool at the moment?** *PROBE ON: Roles, specialisms, specific skill sets (technical and/or complementary), seniority-level* • Why are these roles so difficult to fill? • How, if at all, have you gone about filling these gaps? **How far are AI and automation impacting the market?** • To what extent, if any, are AI cyber security skills being requested by clients? • To what extent, if any, are candidates including AI cyber skills in their CVs? **Approximately, how many active and passive cyber candidates do you have on your books?** • How, if at all, has this changed compared to the past few years? **How long do cyber security staff generally stay in their roles in your experience?** *Probe by seniority (e.g. CISOs)* • Why do you think this is? **How do you go about sourcing cyber candidates?** • What are the most and least effective methods for finding good quality candidates? **To what extent, if any, have your methods of sourcing candidates changed in the past year?** • Why is this? • What lessons, if any, have you learnt?	
4. Diversity of labour market	**10 mins**
What do you think of when we talk about diversity in the cyber sector? What does this refer to? • Why is this? **How diverse is the cyber sector? What kind of diversity do you think is lacking?** • Why is this?	

How, if at all, has this changed / evolved in the last two years? • What specific changes, if any, have you seen? **How would you describe the diversity of the current candidate pool?** • Why have you described it in this way? • How, if at all, has this changed in the past couple of years? **How, if at all, do you diversify the pool of candidates on your books?** • Why do you do it this way? **Have you made any changes in your own approaches and/or behaviours to diversity in the last year?** • *IF SO*, what prompted these changes? • Why did you not implement these changes earlier? • *IF NO CHANGES TO APPROACH*, why not? **What, if anything, would help widen access to the cyber security labour market for different candidates?** • Why have you suggested this? • What steps, if any, have you taken to address this in the past year? • *IF NO STEPS TAKEN*, why not? **How, if at all, do recruitment agencies, such as your own, contribute to this and encourage applicants from different backgrounds and profiles to apply?** • Why is this? **What has been successful? What strategies were less successful?** • Why is this? **What, if any, are typical client demands when it comes to diversity? How, if at all, has this changed in the past year?** • Why is this? **How often, if at all, do clients ask for your guidance when it comes to diversity?** • What sort of responsibility, if any, do recruitment agents have in this area?	
5. Entry-level pathways and expectations	**5 mins**
I would like us to think about entry-level roles in cyber security. What, if any, experience should people thinking about an entry-level role have? • Why is this? **What is the role, if any, of educational institutions in entry-level roles in cyber security? What should their role be?** • Why is this?	

6. Cyber Career Framework and UK Cyber Security Council's professional standards	7 mins
Participants will have been sent a link to the UK Cyber Security Council 16 specialisms and Cyber Career Framework 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: www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/ **What, if anything, had you seen / heard of the 16 cyber security specialisms and the UK Cyber Security Council's Cyber Career Framework before taking part in this research?** **How, if at all, helpful is the Cyber Career Framework?** • How, if at all, is it being used by your cyber team / business? Why is this? • How likely, if at all, would you be to use this resource in your organisation in the future? Why / Why not? • What, if anything, could be added or improved to make it more suitable for your needs? Why have you suggested this? **What impact, if any, could the framework have on developing a shared understanding of cyber roles?** • Why is this? • How, if at all, could it have more impact? Why is this? **What, if anything, do you know about the UK Cyber Security Council's Professional Standards for each of the 16 specialisms?** *IF NECESSARY, EXPLAIN: The UK Cyber Security Council is developing professional standards for each specialism at three levels – associate, principal and chartered.* • What are the advantages and disadvantages of these Professional Standards? • How might this impact recruitment? • What are the implications for your organisation?	
7. Growth areas, emerging opportunities in cyber security	**7 mins**
How do you see the cyber sector evolving in the next 5 years? What factors are going to shape this? • Why do you see it evolving in this way? • Why do you think these factors are going to shape it in this way? **How, if at all, do you foresee your organisation or sector adapting to this evolution?** • Why do you think it will adapt in this way? **What role, if any, will AI and machine learning play in the future of cyber security?** • Why do you see it playing this role?	

Wrap up	2 mins
What is the key thing you would like to feed back to the Department for Science, Innovation and Technology about what we have discussed today? **Is there anything else you'd like to mention that we haven't had a chance to discuss?** **Thank you for your valuable contribution to this important research. Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, which will be taking place again next year. Would you be happy for us to recontact you to take part in this research again? If we were not talking to you, which of your colleagues would we reach out to?** **We would like to keep in touch with recruiters who are happy to take part in this research in the future with updates about our research on cyber security. Would you be happy for us to email you? This would be no more than three or four times a year.** **INCENTIVE**: Thank participant and remind them of confidentiality. Explain that they can get in touch if they have any further comments or questions about the research. Remind them of the £100 as either a bank transfer or charity donation thank you from Ipsos, as an appreciation for their time and contribution to the research. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)	

Appendix F: Topic guide for training providers

Using this guide

The topic guide uses the following conventions: **bold** for questions that should be covered in every interview, bulleted probes for follow-up questions, and *italics* for moderator instructions.

NB When using the guide, the researcher will ask questions and prompts and will use probes to guide where necessary. Probes are asked where the participant does not bring something up spontaneously in response to a question (and the probe is relevant for their particular business). Not all questions or probes will necessarily be used during the interview.

Before each interview: The interviewer will undertake some preparation work including background reading on the participant's organisation and role, as well as the UK Cyber Security Council's Cyber Career Framework (www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/) and Professional Standards (www.ukcybersecuritycouncil.org.uk/professional-standards-registration/).

Introduction	2 - 3 mins
▪ **Introduce yourself and Ipsos**. ▪ **Explain research**: Ipsos carries out an annual study on the cyber security labour market and sector on behalf of the Department for Science, Innovation and Technology (DSIT). This multi-year study has directly informed the government's 2022 to 2025 National Cyber Strategy. You might remember this study from previous years or even have taken part in the research before. As part of the study, we would like to interview training providers like you. This feedback provides us with invaluable information about cyber security skills and training needs in the UK. ▪ **The interview:** The discussion will be informal. There are no right or wrong answers. ▪ **Explain confidentiality**: The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties. ▪ **Explain payment for participation**. You will receive £100 as either a bank transfer or charity donation as a thank you for your time. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.) ▪ **Explain voluntary participation**: If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary. ▪ **Length of the interview**: This discussion will last a maximum of 60 minutes. ▪ **Questions**: Do you have any questions before we begin? ▪ **Consent to audio record**: I would like to record our discussion as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely and deleted 12 months after the interview takes place.	

MODERATOR TO TURN ON RECORDING GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON) Ipsos's legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview and before data is anonymised at the end of November 2024. Can I check that you are happy to proceed?	
1. Business background and context	**2 min**
Firstly, please could you briefly describe your role? • How long have you been working in this organisation / business? • What are your responsibilities? **Please could you briefly tell me about your organisation / business?**	
2. Trends in customer demand	**20 mins**
Can you please describe the current state of the cyber security sector? • Why have you described it in this way? **What, if any, are the biggest challenges you see in cyber security today?** • Why are these the biggest challenges? **In your opinion, what are the most significant market trends currently shaping the cyber security sector?** • Why are these the most significant trends? **Please tell me about the cyber security training that you offer. What are your key areas of focus?** • Why do you offer these? • Why are they your key areas of focus? **Which courses / services are most in demand? How, if at all, has this changed over the last 12 months?** *PROBE ON: numbers of applicants, places / location* • Why is this? **What geography do you offer courses / services over?** • Why do you cover this geography? **How, if at all, do you attract learners to your courses / services?** • Why have you adopted this approach? **What sort of learners are enrolled on your courses?**	

PROBE ON: qualifications, occupation, sector, sponsored by employer or not, reasons for enrolling, diversity **What, if any, challenges do you face in finding suitable learners for your courses?** • Why are these challenges? • How, if at all, do you overcome these challenges? **How do you determine what training to offer?** • What are the key factors? Why are these key factors? • To what extent, if any, are employers informing your course design? **How, if at all, do you work with industry to secure employment outcomes for learners?** **Which particular technologies, if any, are driving demand for training?** • Why is this? **How, if at all, are these technologies being integrated into your courses?** • What, if any, are the challenges in doing this? • *IF CHALLENGES*, how, if at all, are challenges overcomes? **What impact, if any, has AI had on your training?** PROBE ON: both content and delivery • Why has it had this impact? **What training, if any, do you provide for securing AI models and systems?** • Why is this?	
3. Entry-level pathways and expectations	**5 mins**
I would like us to think about entry-level roles in cyber security. What, if any, experience should people thinking about an entry-level role have? • Why is this? **What is the role, if any, of educational institutions in entry-level roles in cyber security? What should their role be?** • Why is this?	
4. Cyber Career Framework and UK Cyber Security Council's professional standards	**7 mins**
Participants will have been sent a link to the UK Cyber Security Council 16 specialisms and Cyber Career Framework 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: www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/	

What, if anything, had you seen / heard of the 16 cyber security specialisms and the UK Cyber Security Council's Cyber Career Framework before taking part in this research? **How, if at all, helpful is the Cyber Career Framework?** • How, if at all, is it being used by your cyber team / business? Why is this? • How likely, if at all, would you be to use this resource in your organisation in the future? Why / Why not? • What, if anything, could be added or improved to make it more suitable for your needs? Why have you suggested this? **What impact, if any, could the framework have on developing a shared understanding of cyber roles?** • Why is this? • How, if at all, could it have more impact? Why is this? **What, if anything, do you know about the UK Cyber Security Council's professional standards for each of the 16 specialisms?** *IF NECESSARY, EXPLAIN: The UK Cyber Security Council is developing professional standards for each specialism at three levels – associate, principal and chartered.* • What are the advantages and disadvantages of these Professional Standards? • How might this impact training? • What are the implications for your organisation?	
5. Diversity of labour market	**5 mins**
What do you think of when we talk about diversity in the cyber sector? What does this refer to? How diverse is the cyber sector? • Why is this? **What kind of diversity do you think is lacking?** • Why is this? **How, if at all, has this changed / evolved in the last two years?** • What specific changes, if any, have you seen?	
6. Growth areas, emerging opportunities in cyber security	**5 mins**
How, if at all, do you see the cyber sector evolving in the next 5 years? What factors are going to shape this? • Why do you see it evolving in this way? • Why do you think these factors are going to shape it in this way? **How, if at all, do you foresee your organisation or sector adapting to this evolution?** • Why do you think it will adapt in this way?	

What role, if any, will AI and machine learning play in the future of cyber security? • Why do you see it playing this role?	
7. New and emerging training areas	**10 mins**
Thinking about the areas the cyber security training you provide focuses on, how, if at all, do you expect this to change over the next 2 to 5 years? • Why is this? **What, if any, are the key factors which will influence any changes in your areas of focus?** • Why is this? **How, if at all, do you expect demand for your courses to change in the next 2 to 5 years? What, if any, factors will shape demand?** • Why is this? **How, if at all, do you see emerging technologies influencing your training?** • Why is this? • Which emerging technologies are likely to have the most impact? Why? • How, if at all, do you plan to adapt your courses / services to incorporate emerging technologies? Why / why not? **What impact, if any, is AI in particular likely to have on training?** *PROBE ON: i) using AI skills in cyber security practices and processes and ii) training on securing AI models and systems?* • Why is this? **What, if any, innovations are taking place in training? What, if any, role can AI play in delivering training?** • Why is this? **What, if any, are gaps or areas for improvement do you see in current cyber security training?** • Why have you suggested this? **What, if any, is the role of educational institutions in ensuring the UK cyber workforce has the skills it requires now and in the future? What, if any, part does industry have to play? And government?** • Why is this?	
Wrap up	**2 mins**
What is the key thing you would like to feed back to the Department for Science, Innovation and Technology about what we have discussed today?	

Is there anything else you'd like to mention that we haven't had a chance to discuss? **Thank you for your valuable contribution to this important research. Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, which will be taking place again next year. Would you be happy for us to recontact you to take part in this research again? If we were not talking to you, which of your colleagues would we reach out to?** **We would like to keep in touch with training providers who are happy to take part in this research in the future with updates about our research on cyber security. Would you be happy for us to email you? This would be no more than three or four times a year.** **INCENTIVE**: Thank participant and remind them of confidentiality. Explain that they can get in touch if they have any further comments or questions about the research. Remind them of the £100 as either a bank transfer or charity donation thank you from Ipsos, as an appreciation for their time and contribution to the research. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)	

Appendix G: Topic guide for investors

Using this guide

The topic guide uses the following conventions: **bold** for questions that should be covered in every interview, bulleted probes for follow-up questions, and *italics* for moderator instructions.

NB When using the guide, the researcher will ask questions and prompts and will use probes to guide where necessary. Probes are asked where the participant does not bring something up spontaneously in response to a question (and the probe is relevant for their particular business). Not all questions or probes will necessarily be used during the interview.

Before each interview: The interviewer will undertake some preparation work including background reading on the participant's organisation and role.

Introduction	2 - 3 mins
• **Introduce yourself and Ipsos** • **Explain research**: Ipsos carries out an annual study on the cyber security sector on behalf of the Department for Science, Innovation and Technology (DSIT). This multi-year study has directly informed the government's 2022 to 2025 National Cyber Strategy. You might remember this study from previous years or even have taken part in the research before. As part of the study, we interview investors in the cyber sector. • **The interview:** The discussion will be informal. There are no right or wrong answers. • **Explain confidentiality**: The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties. • **Explain payment for participation**. You will receive £100 as either a bank transfer or charity donation as a thank you for your time. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.) • **Explain voluntary participation**: If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary. • **Length of the interview**: This discussion will last 45-60 minutes. • **Questions**: Do you have any questions before we begin? • **Consent to audio record**: I would like to record our discussion as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely and deleted 12 months after the interview takes place. *MODERATOR TO TURN ON RECORDING* GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON) Ipsos's legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data	

to be used at any point before, during or after the interview and before data is anonymised at the end of November 2024. Can I check that you are happy to proceed?	
1. Business background and context	**7 min**
Firstly, please could you briefly describe your role? • How long have you been working in this organisation / business? • What are your responsibilities? **Please could you briefly tell me about your business?** • How long has the organisation / business been operating? • What are your main areas of focus? • What is the size and structure of the organisation / business? **Can you briefly summarise your engagement with the UK cyber security sector?** **Which regions do you operate in?** PROBE ON: Inside the UK and outside the UK **How do you find / hear about new investment opportunities in cyber security? How do you stay informed about emerging trends and developments?** *PROBE ON: networks, trade shows, conferences* *PROBE ON: DSIT cyber accelerator schemes, i.e. CyberASAP and Cyber Runway* • How, if at all, do you engage with these accelerator schemes? In what ways? **At what stage of a business (for example, seed, Series A, later-stage) do you typically focus your investments in the cyber security sector?** • Why is this? • What, if any, factors influence this decision? Why is this?	
2.Investor sentiment	**20 mins**
What, if any, types of cyber security companies or solutions are you most interested in investing in currently? *PROBE ON: maturity of business, endorsements, collaborations, time scales, potential, quality / performance of the product / service, market positioning / USP, personnel / personality, market operability* • How, if at all, has this interest changed from previous years? • Why do these types of companies or solutions appeal to you? • What, if any, specific trends or technologies are driving your interest, and how have these evolved? **What are your main criteria for deciding whether to invest in a cyber security business? How, if at all, do you evaluate the potential of cyber security companies or solutions?** *PROBE ON: business plan, networks / collaborators, profit, market trends* • Why are these your main criteria?	

- How, if at all, have these criteria changed compared to previous years? Why is this?
- Why do you evaluate potential in this way?

In which regions or markets are you primarily looking to invest in cyber security? How, if at all, has this focus shifted compared to previous years?

- Why is this?
- Has this changed recently compared to previous years? Why / why not?

How, if at all, does the UK cyber security sector compare to global markets? What concerns or reservations, if any, do you have about investing in UK cyber security companies? How, if at all, do risk / reward considerations differ from other markets?

- Why is this?
- Has this changed recently compared to previous years? Why / why not?

How, if at all, does the cyber sector differ regionally within the UK, and how, if at all, has this changed compared to previous years?

- Why is this?
- Which regions do better?
- Which do worse?
- Why does it differ? *PROBE ON*: investor presence / absence in the region, cyber sector ecosystem

What is your investment time horizon for UK cyber security companies? How, if at all, has this aligned or shifted with your overall investment strategy over the years?

- Why is this?

How, if at all, do you measure the success of your investments in the UK cyber security sector?

- Why do you measure it in this way?

What, if any, are the primary barriers or challenges you face when considering investments in the cyber security sector in the UK, and how have these evolved over the years?

- Why are these considered to be barriers?
- How, if at all, do these barriers compare to those in other global markets and in the UK now compared to before? Why is this?
- What, if any, strategies do you see to overcome these barriers? Why have you chosen these strategies?

What are your thoughts on the current state of regulation in the UK cyber security industry and its impact on investment decisions? How, if at all, has this regulatory landscape changed over the years?

- Why is this?

How do you view the role of the UK government and regulatory bodies in shaping the cyber security investment landscape now, compared to previous years? • Why is this? **In your view, how, if at all, has the cyber security investment landscape changed within the last twelve months?** *PROBE BY: firm, level of investment, macroeconomic factors (for example, inflation)*	
3. Growth enablers for sector (including skills)	**10 mins**
What, if any, are the most significant factors driving the growth of the cyber sector today? • Why are they the most significant factors? • How, if at all, do these factors compare to previous years? • Are there any newer or bigger factors emerging? **What specific technological advancements, if any, are contributing towards this growth?** • Why are they contributing towards this growth? **What, if anything, is hindering the growth of the cyber sector? What steps, if any, can be taken to mitigate these challenges?** *PROBE ON: TECHNICAL/REGULATORY/VALUATION CHALLENGES, AVAILABILITY OF SKILLS* • Why is this? • Are there any new challenges emerging compared to previous years? How, if at all, can these newer challenges be mitigated? **What steps can cyber security companies take to make themselves more attractive to investors? Why?**	
4. Growth areas, emerging opportunities in cyber security	**10 mins**
I'd now like us to think about the future. What, if any, are your expectations for the future growth and profitability of the UK cyber security industry? **How do you assess the long-term growth potential of the cyber sector?** • Why do you have these expectations? **What factors, in your view, will drive or hinder this long-term growth?** • Why is this? **What, if any, types of cyber security firm do you think will gain most attention from investors (or buyers) in the coming years?** *PROBE ON: types of firms / products / services, subsectors and domains, for example, role of cyber security in defence / deep tech, emerging technologies* • Why is this?	

What, if any, specific attributes or characteristics will you be looking for in cyber businesses in the coming years? • Why is this? **What are your expectations regarding the availability and cost of skilled cyber professionals in the coming years? How, if at all, might these factors impact the growth and profitability of cyber companies? How, if at all, important is a company's approach to talent acquisition and development when evaluating cyber investment opportunities?** • Why is this? **What, if any, impact do you believe artificial intelligence (AI) and machine learning (ML) will have on the UK cyber security industry and your investment decisions? What other technologies may impact future growth in the sector?** *PROBE ON ANY SPECIFIC TECHOLOGIES MENTIONED IN THE PREVIOUS SECTION* • Why is this?	
Wrap up	**5 mins**
What is the key thing you would like to feed back to the Department for Science, Innovation and Technology about what we have discussed today? **Is there anything else you'd like to mention that we haven't had a chance to discuss?** **Thank you for your valuable contribution to this important research. Ipsos and Perspective Economics are undertaking this work as a multi-year study for DSIT, which will be taking place again next year. Would you be happy for us to recontact you to take part in this research again? If we were not talking to you, which of your colleagues would we reach out to?** **We would like to keep in touch with investors who are happy to take part in this research in the future with updates about our research on cyber security. Would you be happy for us to email you? This would be no more than three or four times a year.** **INCENTIVE**: Thank participant and remind them of confidentiality. Explain that they can get in touch if they have any further comments or questions about the research. Remind them of the £100 as either a bank transfer or charity donation thank you from Ipsos, as an appreciation for their time and contribution to the research. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)	

Appendix H: Inclusion/exclusion criteria for job vacancies analysis

We developed the search string below to identify job postings for technical cyber security job role and cyber-enabled roles on the Lightcast 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 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 (Core Cyber Security Roles)

Roles containing any of the selected skills: "cyber" (29 matches), "information security" (25 matches), Application Security Testing, Cloud Security Infrastructure, CompTIA IT Fundamentals (ITF+), Computer Security, Digital Security, Endpoint Security, IT Security Architecture, IT Security Documentation, ITIL Security Management, Microsoft Security Essentials, Network Security, Network Security Policy, Network Security Specialist, Operational Technology (OT) Security, Security Controls, Security Technology, Software Security, Web Application Security, WiFi Security, Wireless Security And CONTRACT_TYPE=”Permanent” AND POSTING_TYPE=”Newly Posted” And EXCLUDE job titles containing… "accountant" (280 matches), "cctv" (2 matches), "entry" (67 matches), "finance" (302 matches), "fire" (106 matches), "solicitor" (10 matches), "trainee" (118 matches), Account Managers, Azure Engineers, Business Analysts, Business Delivery Specialists, Business Department Chairs, Business Designers, Business Developer Managers, Business Developers, Business Development Account Executives, Business Development Account Managers, Business Development Account Representatives, Business Development Administrative Assistants, Business Development Administrators, Business Development Executives, Business Development Managers, Core Network Engineers, Data Scientists, DevOps Engineers, DevSecOps Engineers, Embedded Software Engineers, Front End Developers, Full Stack, Developers, Infrastructure Engineers, Infrastructure Managers, IT Auditors, IT Managers, IT Support Engineers, IT, Support Technicians, Java Developers, Lecturers, Lecturers in Computer Science, Line Support Engineers, Network Engineers, Recruitment Consultants, Sales Development Representatives, Software Developers, Software Engineers And EXCLUDE occupations containing… Account Manager / Representative, Accountant, Actuary, Administration, Manager, Advertising Sales Representative, Alarm / Security System Technician, Asset Protection / Security, Manager, Auditor, Bookkeeper / Accounting Clerk, Business / Management Analyst, Business Continuity Planner / Analyst, Business Development Executive, Business Intelligence Architect / Developer, Civil Engineer, Clinical Coder, Computer Programmer, Computer Support Specialist, Computer Systems Engineer / Architect, Credit Analyst / Authoriser, Customer Service Manager, Customer Service Representative, Data / Data Mining Analyst, Data Engineer, Data Warehousing Specialist, Database Administrator, Database Architect, Door - to - Door Sales Worker, Driving instructors, Electrical Engineer, Emergency Management Director, Financial Analyst, Financial Manager, Financial Services Sales Agent, Human Resources / Labour Relations Specialist, Human Resources Manager, Industrial Engineer, Insurance Sales Agent, Lawyer, Logistics / Supply Chain Analyst, Market Research Analyst, Marketing Coordinator / Assistant, Marketing Manager, Marketing Representative, Marketing Specialist, Mechanical Engineer, Mechatronics Engineer, Medical / Pharmaceutical Sales Representative, Membership Sales Representative, Network / Systems Administrator, Network / Systems Support Specialist, Office / Administrative Assistant, Operations Analyst, Parts Specialist / Salesperson, Personal Banker / Banking Sales Staff, Procurement Manager, Production Worker, Quality Control Analyst, Recruiter, Repair / Service Technician, Retail Sales Associate, Route Sales Representative, Sales Assistant, Sales Consultant, Sales Delivery Driver, Sales Engineer, Sales Manager, Sales Representative, Sales Supervisor, Scheduler / Operations Coordinator, Search Engine Optimisation Specialist, Security Officer, Senior Administrator, Sheet Metal Fabricator / Mechanic, Software Developer / Engineer, Software QA Engineer / Tester, Solar Sales Representative, Stocking Clerk / Sales Floor Support, Storage / Distribution Manager, Technical Sales Representative, Technical Writer, Transportation Security Officer, Tutor, UI / UX Designer, University Lecturer, Utilities Technician, Validation Engineer, Web Designer, Web Developer

Search Strategy (**ALL Cyber Security Roles**)

Roles containing any of the selected skills: "cyber" (29 matches), "information security" (25 matches), Application Security Testing, Cloud Security Infrastructure, CompTIA IT Fundamentals (ITF+), Computer Security, Digital Security, Endpoint Security, IT Security Architecture, IT Security Documentation, ITIL Security Management, Microsoft Security Essentials, Network Security, Network Security Policy, Network Security Specialist, Operational Technology (OT) Security, Security Controls, Security Technology, Software Security, Web Application Security, WiFi Security, Wireless Security AND POSTING_TYPE=”Newly Posted”

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.