Ipsos MORI
Social Research Institute

Understanding the UK cyber security skills labour market

Technical report

Dr Sarah Fullick, Daniel Pedley, Darragh McHenry, Helen Motha and Jayesh Navin Shah

Contents

1 Overview

The UK Government Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos MORI and the Institute of Criminal Justice Studies (ICJS) at the University of Portsmouth to carry out quantitative and qualitative research to better understand the current state of the UK cyber security skills labour market. The work forms part of the UK Government's National Cyber Security Strategy 2016 to 2021[1]. The £1.9 billion investment taking place under this strategy aims, alongside other objectives, to ensure the UK has a sustainable supply of home-grown cyber professionals to meet the growing demands of an increasingly digital economy, in the public and private sectors, and in defence. This research is intended to inform DCMS's strategic vision and programmes of activity on cyber security skills development.

This report provides the technical details for all strands of the research project, and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings. DCMS has published a separate report of the main findings from the research.[2]

1.1 Summary of methodology

The methodology consisted of four strands, as outlined here. The first two strands fed into the development of the quantitative survey, and the results from the survey fed into the follow-up qualitative interviews.

1. Professor Mark Button and Dr Victoria Wang from ICJS carried out a rapid evidence review of 32 existing evidence sources (surveys and white papers, globally and in the UK). We include a full list of sources in Appendix A. Ipsos MORI carried out the remaining strands.
2. We carried out 12 in-depth interviews with industry experts representing a range of trade associations, multinational businesses, cyber security specialists, training providers, recruitment agencies, academics and Government. These took place in March and April 2018.
3. We conducted a quantitative survey of 1,030 businesses, 127 public sector organisations and 470 charities from 12 June to 6 August 2018. Survey data are weighted to be representative of these respective audiences. The business sample excludes agriculture, forestry and fishing businesses. The public sector sample excludes parish councils and central Government Departments.[3]
4. We carried out 32 further in-depth interviews, including 27 with a mix of organisations that took part in the survey and 5 with external cyber security providers that were not in the survey. External cyber security providers are those that offer IT or cyber security services to other organisations.

[1] See https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

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

[3] DCMS decided that agriculture, forestry and fishing businesses would be less likely to have IT capacity or an online presence. We would typically have screened such organisations out of the survey, so we excluded them from the sample instead. This matches the approach taken in DCMS's Cyber Security Breaches Survey series. We excluded parish councils because larger public sector organisations were a greater priority for DCMS. If included, the volume of parish councils means that the public sector sample would have been dominated just by these. Finally, in agreement with DCMS, we ensured that central Government Departments were not on the sample, as we anticipated they would not be able to take part, or share sensitive information.

2 Scoping research

2.1 Rapid evidence review

Professor Mark Button and Dr Victoria Wang from ICJS led this initial strand of the research in March and April 2018. It aimed to pull together the most important existing evidence on the cyber security skills gap, with a particular focus on the following objectives:

- existing definitions or categorisations of cyber security skills
- existing frameworks of cyber security job roles
- the state of the current UK cyber skills labour market and common recruitment practices
- evidence and best practice from the UK and other nations in addressing cyber security skills gaps
- implications for the quantitative survey, in terms of evidence gaps and relevant question areas.

ICJS drew up a longlist of documents to potentially include in the review, all from within the last five years, since 2013. They found these through a mix of:

- general online searching with key terms such as "cyber security skills" and "cyber security labour market"
- targeted searching on Government websites (in the UK and other developed nations) and in parliamentary evidence submissions
- known global surveys, such as the ISC2 Cybersecurity Workforce Study (formerly known as the Global Information Security Workforce Studies, or GISWS, last published in 2018 under Frost & Sullivan), the Centre for Strategic and International Studies (CSIS, 2016) survey, and the annual ISACA surveys (last published in 2018).

DCMS and Ipsos MORI added to this longlist, and DCMS highlighted the documents that they considered essential to include in the review, focusing especially on the most recent publications. As the project as a whole progressed, DCMS highlighted a small number of new sources of evidence published along the way, and ICJS added these to the review. The shortlist of 32 sources included in the final review, following these minor updates, is in Appendix A.

We made various observations about the existing literature, that highlighted the lack of a reliable existing evidence base for cyber security skills gaps in the UK:

- Several of the shortlisted reports did not contain primary research, but were instead summarising or collating research from other shortlisted sources. For example, the Silensec (2017) report draws upon the CSIS (2016) survey and ISACA (2017a and 2017b) surveys, and Cobb (2018) refers frequently to the former GISWS surveys. Therefore, the primary research data on this topic is very limited, to a small number of regularly-referenced sources.
- Several reports had a global focus, or focused on the US or Europe, as opposed to the UK.
- Many of the organisations sponsoring the reports that highlighted or forecast cyber security skills gaps and shortages also had vested interests, as they offered cyber security products and services to clients (this is noted in Cobb, 2016).

Following this stage, ICJS drafted an internal literature review report for DCMS and Ipsos MORI. This included a list of recommendations for the quantitative survey, in terms of audiences to include and key question areas. This then fed into Ipsos MORI's development of the survey.

2.2 Industry expert interviews

Ipsos MORI carried out in-depth telephone interviews with 12 industry experts between March and April 2018. The purpose of this stage of the research was to get expert opinions, beyond the existing literature, on:

- the state of the current UK cyber security skills labour market – the types of organisations requiring cyber security skills, the types of cyber security job roles in the market, and the types of job roles with skills shortages
- the types of training products, recruitment services and other solutions that organisations might be using to meet their cyber security skills needs, and what kinds of products or services are available or lacking in the current market
- early suggestions of key lessons and recommendations on what the Government and industry can do to tackle the cyber security skills gap, which could be further probed in later qualitative interviews with organisations.

The experts came from a mix of business representative organisations, cyber security product or service providers, training providers, recruitment agencies, academics working in the field of cyber security and Government bodies. We sourced participants from existing DCMS and ICJS contacts, as well as business representative organisations that had previously participated in DCMS/Ipsos MORI scoping research for the Cyber Security Breaches Survey series (2016–2018).[4]

Interviews lasted c.45 minutes. We recorded each interview and wrote detailed notes for each one with the key discussion points and themes highlighted. We discussed these findings verbally with the DCMS project team, and also provided a written summary as an annex to ICJS's internal literature review report. This then fed into the quantitative survey development, particularly in terms of categorising cyber security skills for measuring skills gaps in the questionnaire – by merging key themes from these interviews with those from the rapid evidence review, and important existing frameworks such as the Cyber Security Body of Knowledge (CyBOK).[5] We also asked participants from this stage to review a draft of the questionnaire and comment on it, to feed into the final version.

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

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

3 Survey approach technical details

3.1 Survey and questionnaire development

Ipsos MORI developed the questionnaire and all the other survey instruments (such as interviewer instructions, a reassurance email for respondents and a survey website page), building in key themes from the existing literature and industry expert interviews. Development took place over two stages, and DCMS approved the questionnaire at each stage:

- cognitive testing interviews with 8 businesses, charities and public sector organisations
- a pilot survey, consisting of 40 interviews with these three types of organisations.

Cognitive testing

We carried out cognitive testing interviews from 2 to 11 May 2018. The 8 participating organisations included 2 businesses, 4 charities and 2 public sector organisations. Across these, there was a mix by size (measured in terms of number of employees for businesses and public sector organisations, and income band for charities) and sector. We applied quotas at the recruitment stage by size, sector and region to ensure this mix.

The cognitive testing was intended to test:

- who the most appropriate individual within an organisation to survey would be
- comprehension of the questions and any technical terms used
- the user-friendliness of the reassurance email
- the kinds of messages and non-financial incentives (such as receiving a copy of the report) that might encourage respondents to take part in the main survey.

We recruited participants by telephone, using sample purchased from the Experian business database (for businesses and public sector organisations), as well as the Charity Commission for England and Wales charity database (charities from Scotland and Northern Ireland were not included in this phase but were included in the subsequent phases of the research). All participants received a £40 incentive from Ipsos MORI to ensure different-sized businesses from a range of sectors took part.[6]

In terms of the individuals we recruited within each organisation, we tested two approaches. One targeted the hiring managers or other senior individuals most responsible for making decisions around recruitment, considering that they might be more capable than others of talking about the organisation's skills shortages. Another targeted the individual with most direct responsibility for cyber security in the organisation, as they would potentially be best placed to talk about the technical aspects of their role. We found early on that the second approach was far more productive, as several organisations were simply not hiring people in cyber security roles and the individuals in charge of such decisions, when they did not directly work in a cyber security role, could not identify the organisation's cyber security skills needs very well. Interviewing the senior lead most directly responsible for cyber security is the approach we took in the main survey.

After this stage, we amended the questionnaire and other survey instruments to reflect the cognitive testing feedback. The main changes included:

- amending the phrase "incident response" into plainer English, as "dealing with cyber attacks"

[6] This was administered either as a cheque to the participant or as a charity donation, as the participant preferred.

- removing certain questions about the knowledge and behaviour of senior managers or wider staff, which respondents in cyber security roles simply were not able to answer
- making the questionnaire better suited to public sector organisations, where respondents were unable to answer questions around turnover, and, anecdotally, we found they had greater concerns about confidentiality.

Pilot survey

We carried out a short pilot survey to:

- time the questionnaire
- gather further feedback on the survey introductory text and reassurance email
- test the usefulness of the written interviewer instructions
- examine the quality of the sample.

Fieldwork took place from 29 May to 4 June 2018. Again, we applied quotas to ensure the pilot covered different-sized businesses from a range of sectors, different-sized public sector organisations, and charities with different incomes.

The pilot sample was taken from the same sample frames used for the main stage survey (see Section 3.2). In total, 560 leads were randomly selected, with 381 identified as eligible. Not all of these leads were used to complete the 40 pilot interviews. In total, 11 businesses, 17 charities and 12 public sector organisations, and 179 untouched leads were re-released for use in the main survey.

Of the 12 public sector organisations, 10 turned out to be parish councils. This highlighted the issue that the public sector, considering each organisation as a single sampling unit, is largely made up of parish councils – micro organisations that are the smallest tier of local government. If we included parish councils in the main survey, the achieved public sector sample would overwhelmingly be composed of these types of organisations. Parish councils were of far less strategic importance to DCMS than NHS organisations, schools or larger local authorities, so Ipsos MORI and DCMS jointly agreed at the pilot stage that we would exclude all parish councils from the main survey sample.

The main questionnaire changes we made following the pilot survey were as follows:

- cuts to bring the questionnaire length down to within c.17–18 minutes for the main stage. This included scripting some questions to only be asked on half of respondents to reduce questionnaire length on average.
- new precodes added for unprompted questions to reflect common "other" verbatim responses.

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

3.2 Sampling

The target population included:

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

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

Business and public sector sample frame

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

Charity sample frames

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: http://data.charitycommission.gov.uk/default.aspx
- the Scottish Charity Regulator database: https://www.oscr.org.uk/about-charities/search-the-register/charity-register-download
- the Charity Commission for Northern Ireland database: https://www.charitycommissionni.org.uk/charity-search/.

Again, this approach is consistent with the DCMS/Ipsos MORI Cyber Security Breaches Survey series.

In England and Wales, and in Scotland, the respective charity regulator databases contain a comprehensive list of registered charities. The Charity Commission in Northern Ireland does not have a comprehensive list of established charities. It is in the process of registering charities and building one. We considered and ruled out alternative sample frames for Northern Ireland, such as the Experian and Dun & Bradstreet business directories (which also include charities), because they did not contain essential information on charity income for sampling, and cannot guarantee up-to-date charity information.

Therefore, while the Charity Commission in Northern Ireland database was the best sample frame for this survey, it cannot be considered as a truly random sample of Northern Ireland charities at present. This situation is set to improve for future surveys, as the database becomes more comprehensive.

Sample selection

In total, we selected 37,871 businesses and public sector organisations from the IDBR, with proportionate stratification by sector, and disproportionate stratification by size. The disproportionate stratification by size reflects the intention to carry out subgroup analysis by the size of the business. This would not be possible with a proportionate stratification (which would effectively exclude any meaningful number of medium and large businesses from the selected sample). Table 3.1 breaks down the selected sample by size and sector.

Table 3.1: Pre-cleaning selected business sample by size and sector

SIC 2007 letter[7]	Sector description	Micro or small (1–49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
B, C, D, E	Utilities or production (including manufacturing)	1,098	243	361	1,702
F	Construction	3,125	38	51	3,214

[7] SIC sectors here and in subsequent tables in this report have been combined into the sector groupings used in the main report.

G	Retail or wholesale (including vehicle sales and repairs)	2,059	83	220	2,362
H	Transport or storage	1,219	28	65	1,312
I	Food or hospitality	1,573	66	78	1,717
J	Information or communications	8,157	170	278	8,605
K	Finance or insurance	774	206	390	1,370
L, N	Administration or real estate	3,228	71	210	3,509
M	Professional, scientific or technical	4,253	59	138	4,450
O	Other public sector	2,822	135	120	3,077
P	Education (including academies)	2,676	121	162	2,959
Q	Health, social care or social work (including NHS)	2,183	194	146	2,523
R, S	Entertainment, service or membership organisations	1,017	18	36	1,071
	Total	34,184	1,432	2,255	37,871

The charity sample was proportionately stratified by country and disproportionately stratified by income band. This used the same reasoning as for businesses – without this disproportionate stratification, analysis by income band would not be possible as hardly any high-income charities would be in the selected sample. As the entirety of the three 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 3.1 is shown for charities.

Sample telephone tracing and cleaning

Not all the original sample was usable. In total, 25,954 original business leads had either no telephone number or an invalid telephone number (i.e. the number was either in an incorrect format, too long, too short or a free phone number which would charge the respondent when called). For Scottish charities, there were no telephone numbers at all on the database.

We carried out telephone tracing through the UK Changes database (matching to both business and, for micro businesses and charities, residential number databases) to fill in the gaps where possible. No telephone tracing was required for charities from England and Wales, and Northern Ireland.

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

Following telephone tracing and cleaning, the usable business sample amounted to 11,917 leads (including the leads taken forward from the pilot). For the Scotland charities sample, 1,973 leads had telephone numbers after matching.

Table 3.2 breaks the business leads down by size and sector.

Table 3.2: Post-cleaning available main stage sample by size and sector

SIC 2007 letter	Sector description	Micro or small (1–49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
B, C, D, E	Utilities or production (including manufacturing)	475	234	343	1,052
F	Construction	982	30	51	1,063
G	Retail or wholesale (including vehicle sales and repairs)	708	76	206	990
H	Transport or storage	265	24	60	349
I	Food or hospitality	442	52	71	565
J	Information or communications	1,589	141	239	1,969
K	Finance or insurance	513	183	348	1,044
L, N	Administration or real estate	849	59	186	1,094
M	Professional, scientific or technical	1,042	45	112	1,199
O	Other public sector	58	117	112	287
P	Education (including academies)	778	91	133	1,002
Q	Health, social care or social work (including NHS)	598	173	133	904
R, S	Entertainment, service or membership organisations	355	14	30	399
	Total	8,654	1,239	2,024	11,917

The usable leads for the main stage survey were randomly allocated into separate batches for businesses and charities. The first business batch included 4,203 leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band from the three previous surveys in the DCMS/Ipsos MORI Cyber Security Breaches Survey series. In other words, we selected more sample in sectors and size bands where there was a higher target, or where response rates were relatively low last year. The first charity batch had 1,557 leads matching the disproportionate targets by income band.

We drew up and released subsequent batches of sample as and when the live sample was exhausted. Not all available leads were released in the main stage (see Tables 3.3 and 3.4 for the total sample loaded).

3.3 Fieldwork

Main stage fieldwork was carried out from 12 June to 6 August 2018 using a Computer-Assisted Telephone Interviewing (CATI) script.

In total, we completed 1,627 interviews, comprising 1,030 businesses (excluding agriculture, forestry and fishing businesses), 127 public sector organisations (excluding parish councils), and 470 registered charities. The average interview length was c.18 minutes.

Fieldwork preparation

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

- written instructions about all aspects of the survey
- a copy of the questionnaire and other survey instruments
- the glossary of unfamiliar terms.

Screening of respondents

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

- organisations with no computer, website or other online presence (interviewers were briefed to probe fully before coding this outcome, and it was used only in a small minority of cases)
- organisations that identified themselves as sole traders with no other employees on the payroll[8].

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.

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

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

Random-probability approach and maximising participation

We adopted random-probability sampling to minimise selection bias. The overall aim with this approach is to have a known outcome for every piece of sample loaded. For this survey, we used an approach comparable to other robust business surveys – including the DCMS/Ipsos MORI Cyber Security Breaches Surveys – around this:

- We called each piece of sample either a minimum of 7 times, or until we achieved an interview, received a refusal, or received enough information to make a judgment on the eligibility of that contact. Typically, we actually called leads 10 or more times (e.g. when respondents had requested to be called back at an early stage in fieldwork but had subsequently not been reached).
- Each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. We also offered evening and weekend interviews on request to respondents.

Several steps were taken to maximise participation in the survey and reduce non-response bias. Interviewers could send the reassurance email to prospective participants to confirm the legitimacy of the study, and provide more information.

[8] These are typically excluded for business surveys of this nature as many of the questions asked would not be applicable or relevant to them.

Fieldwork monitoring

Ipsos MORI is a member of the interviewer Quality Control Scheme recognised by the Market Research Society. In accordance with this scheme, the field supervisor on this project listened into at least 10 per cent of the interviews and checked the data entry on screen for these interviews.

3.4 Fieldwork outcomes and response rate

The Ipsos MORI research team monitored fieldwork outcomes and response rates throughout fieldwork and gave interviewers regular guidance on how to avoid common reasons for refusal. Table 3.3 shows the final outcomes and the adjusted response rate calculation for business and public sector, and Table 3.4 shows the final outcomes and the adjusted response rate calculation.[9]

With this survey it is especially important to bear in mind that fieldwork overlapped with the Christmas and New Year sales periods. While fieldwork was managed to frontload calls to sectors that were likely to be less available over these periods (e.g. retail and wholesale businesses), this timing still made it considerably challenging to reach participants, which will have affected the final response rate.

Table 3.3: Fieldwork outcomes and response rate calculations for businesses and public organisations

Outcome	Total
Total sample loaded	8,023
Completed interviews	1,157
Incomplete interviews	36
Ineligible leads – established during screener[10]	405
Ineligible leads – established pre-screener	151
Refusals	1,199
Unusable leads with working numbers[11]	735
Unusable numbers[12]	813
Working numbers with unknown eligibility[13]	3,527
Expected eligibility of screened respondents[14]	75%

[9] The adjusted response rate with estimated eligibility has been calculated as: completed interviews / (completed interviews + incomplete interviews + refusals + any working numbers expected to be eligible). It adjusts for the ineligible proportion of the total sample used. Expected eligibility has been calculated as: (completed interviews + incomplete interviews + refusals) / (completed interviews + incomplete interviews + refusals + ineligible leads + unusable leads with working numbers).

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

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

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

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

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

Expected eligibility of working numbers[15]	57%
Unadjusted response rate	14%
Adjusted response rate	28%

Table 3.4: Fieldwork outcomes and response rate calculations for charities

Outcome	Total
Total sample loaded	1,582
Completed interviews	470
Incomplete interviews	17
Ineligible leads – established during screener	24
Ineligible leads – established pre-screener	61
Refusals	136
Unusable leads with working numbers	136
Unusable numbers	93
Working numbers with unknown eligibility	645
Expected eligibility of screened respondents	95%
Expected eligibility of working numbers	73%
Unadjusted response rate	30%
Adjusted response rate	43%

3.5 Data processing and weighting

Sample versus questionnaire information

To split out private, public and charitable sector organisations, we used a mix of questionnaire and sample information. For charities sampled from their respective charity regulator databases, we assumed based on the sample frame that these were definitely charities. For organisations sampled from the IDBR, we instead allowed them to self-identify as either a private sector organisation, public sector organisation or charity, and only used sample information if they did not answer this question in the interview.

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

Coding

The verbatim responses to unprompted questions could be coded as "other" by interviewers when they did not appear to fit into the predefined code frame. Ipsos MORI's coding team coded these "other" responses manually, and where possible, assigned them to codes in the existing code frame. It was also possible for new codes to be added where

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

enough respondents – 10 per cent or more – had given a similar answer outside of the existing code frame. The accuracy of the coding was verified by the Ipsos MORI research team, who checked and approved each new code proposed.

We did not undertake SIC coding. Instead, we used the SIC 2007 codes that were already in the IDBR sample to assign businesses to a sector for weighting and analysis purposes. This is the same approach as in the DCMS/Ipsos MORI Cyber Security Breaches Surveys. See the main report for the full list of SIC 2007 codes.

Weighting

We applied rim weighting (random iterative method weighting) to account where possible for non-response bias and also to account for the disproportionate sampling of businesses by size. The intention was to make the final reported data representative of the actual UK business, public sector and registered charity populations. 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. The same weighting approach is used in the DCMS/Ipsos MORI Cyber Security Breaches Surveys.

We used four separate weighting schemes:

1. For businesses, there were non-interlocking weights by size and sector, based on the population profile in the 2017 Department for Business, Energy and Industrial Strategy (BEIS) business population estimates (the latest ones published at the time of fieldwork).[16] We did not weight by region but it should be noted that the final weighted data are closely aligned with the regional profile of the population. Interlocking weighting 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 at each question.

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 2017 BEIS business population estimates.

4. One complexity in the weighting of private and public sector organisations is that certain sectors of the economy contain a mix of the private and public sector – especially education (SIC sector P) and health (SIC sector Q). For analysing these two sector subgroups, we created a fourth weighting scheme that merged the private and public sector population profiles from the 2017 BEIS estimates.

Tables 3.5, 3.6, 3.7 and 3.8 show the unweighted and weighted profiles of the final data, across the 4 weighting schemes.

Table 3.5: Unweighted and weighted sample profiles for businesses (excluding industry sectors that contain both private and public sector organisations)

	Unweighted %	Weighted %
Size		
Micro or small (1–49 staff)	70%	97%
Medium (49–249 staff)	19%	3%
Large (250+ staff)	11%	1%

[16] See https://www.gov.uk/government/statistics/business-population-estimates-2017.

	Unweighted %	Weighted %
Sector		
Administration or real estate	8%	12%
Construction	7%	12%
Entertainment, service or membership organisations	4%	7%
Finance or insurance	10%	2%
Food or hospitality	6%	10%
Information or communications	12%	6%
Professional, scientific or technical	9%	15%
Retail or wholesale	13%	18%
Transport or storage	4%	3%
Utilities or production (including manufacturing)	12%	7%
Region		
East Midlands	7%	7%
Eastern	10%	13%
London	16%	12%
North East	3%	3%
North West	9%	9%
Northern Ireland	4%	5%
Scotland	6%	7%
South East	15%	16%
South West	9%	10%
Wales	4%	4%
West Midlands	9%	7%
Yorkshire and Humberside	7%	7%

Table 3.6: Unweighted and weighted sample profiles for charities

	Unweighted %	Weighted %
Size		
£0 to under £100,000	38%	65%
£100,000 to under £500,000	19%	19%
£500,000 or more	41%	15%
Country		
England and Wales	85%	85%
Scotland	5%	12%
Northern Ireland	10%	3%

Table 3.7: Unweighted and weighted sample profiles for public sector organisations and industry sectors that contain both private and public sector organisations (using merged weighting scheme)

	Unweighted %	Weighted %
Size		
Micro or small (1–49 staff)	2%	2%
Medium (49–249 staff)	20%	26%
Large (250+ staff)	78%	71%

Table 3.8: Unweighted and weighted sample profiles for industry sectors that contain both private and public sector organisations (using merged weighting scheme)

	Unweighted %	Weighted %
Sector		
Education (including academies)	9%	2%
Health, social care or social work (including NHS)	10%	5%

4 Qualitative approach technical details

4.1 Sampling

We carried out 32 in-depth interviews. Of these, the sample for 27 organisations came from those participating in the survey, who had agreed to recontact. In total, 674 (41%) agreed to be recontacted in the survey. This included:

- 12 businesses
- 6 public sector organisations
- 9 charities.

We recruited a further 5 interviews with external cyber security providers, who provide cyber security products or services for others, and these were recruited through DCMS contacts passed to Ipsos MORI.

4.2 Recruitment and quotas

Recruitment was carried out by telephone. Ipsos MORI offered a £50 incentive[17] to encourage participation.

We applied soft recruitment quotas to ensure that the 27 private, public or charitable sector interviews included a mix of:

- different sizes, sectors and regions
- organisations that outsourced some aspects of cyber security (10 of the 27)
- those that had previously recruited for a cyber security role (10)
- those where staff had formal cyber security qualifications (11)
- those that had sought cyber security training (18 had sought training for staff in cyber security roles, and 10 had sought training for wider staff)
- those that covered cyber security both formally (10) and informally (17).

Early in fieldwork, we realised that interviews with smaller organisations were relatively unproductive, given their relative lack of knowledge and understanding of the technical complexities of cyber security. Therefore, later interviews were more heavily weighted towards larger organisations with more sophisticated cyber security needs.

4.3 Fieldwork

The Ipsos MORI research team carried out all the telephone fieldwork in July and August 2018. Interviews lasted c.45 minutes on average.

The interview topic guide was drafted by Ipsos MORI and was approved by DCMS. Later on, during fieldwork, we adapted the topic guide to work specifically for external cyber security providers. Both versions of the guide covered the following:

- What do organisations define as a cyber security skill and how do they differentiate these from IT skills?
- Who makes decisions around cyber security, and how did these individuals enter the role?
- What outsourcing arrangements do organisations have in place, and how confident are they in managing arrangements with external product or service providers?
- What cyber security skills are different types of organisations recruiting for, and what soft and technical skills are organisations looking for in recruitment? How are they going about recruitment?

[17] This was administered either as a cheque to the participant or as a charity donation, as the participant preferred.

- Do the skills in the market meet the needs of organisations?
- What does good practice in terms of training and upskilling look like? Do the available training products and resources meet industry needs?
- Are there any recommendations for the Government or the cyber security industry?

The original topic guide is included in Appendix C. As with any qualitative topic guide, we did not ask the prompts and probes on this guide word-for-word in each interview. Instead, we used it as a starting point to hold discussions with the interview participants – only one interview was with a small business and only one interview was with a charity with under £100,000 in annual income.

4.4 Analysis

Interviews were summarised in a notes template. Throughout fieldwork, the core research team discussed interim findings and outlined areas to focus on in subsequent interviews. DCMS also attended or listened into some of these discussions. At the end of fieldwork, we drew out key themes and case studies in a final face-to-face analysis meeting.

Appendix A: references

Button and Cross (2017) Cyber Frauds, Scams and their Victims (https://www.routledge.com/Cyber-Frauds-Scams-and-their-Victims/Button-Cross/p/book/9781138931206)

Capgemini Digital Transformation Institute (2018) Cyber Security Talent: The Big Gap in Cyber Protection (https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf)

Centre for Strategic and International Studies (2016) Hacking the Skills Shortage, McAfee (https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf)

Cisco (2015) Mitigating the Cyber Skills Shortage (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf)

Cobb (2016) Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis (https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf)

Cobb (2018) "Plugging the skills gap: the vital role that women should play in cyber-security", Computer Fraud & Security, 2018(1), pp.5-8 (https://www.sciencedirect.com/science/article/pii/S1361372318300046)

Dallaway (2016) Closing the Gap in Cyber Security (http://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf)

Ecorys UK (2016) Digital skills for the UK economy, Department for Digital, Culture, Media and Sport (https://www.gov.uk/government/publications/digital-skills-for-the-uk-economy)

Frost & Sullivan (2017) Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk (https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf)

Frost & Sullivan (2017) The 2017 Global Information Security Workforce Study Women in Cyber Security (https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf)

Furnell, Fischer and Finch (2017) "Can't get the staff? The growing need for cyber-security skills", Computer Fraud & Security, 2017(2), pp.5-10 (https://www.infona.pl/resource/bwmeta1.element.elsevier-a6d11d51-060b-324d-bd4b-d7e6e7a549e7)

Geraghty, Ladner, Nana and Peterson (2016) Understanding the Cybersecurity Labor Market: A Primer for CNA Analysis and Solutions (https://www.cna.org/cna_files/pdf/DRM-2016-U-013905-Final.pdf)

Gjersoe (2018) "Bridging the gender gap: why do so few girls study Stem subjects?" The Guardian (https://www.theguardian.com/science/head-quarters/2018/mar/08/bridging-the-gender-gap-why-do-so-few-girls-study-stem-subjects)

HM Government (2016) National Cyber Security Strategy 2016-2021 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)

Information Assurance Advisory Council (2017) The profession: understanding careers and professionalism in cyber security (http://www.iaac.org.uk/wp-content/uploads/2018/02/2017-03-06-IAAC-cyber-profession-FINAL-Feb18-amend-1.pdf)

Inspired Careers website (viewed in August 2018) (https://www.inspiredcareers.org/browse-careers/cyber-security/)

Ipsos MORI (2018) Cyber Security Breaches Survey 2018: Main report, Department for Digital, Culture, Media and Sport (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018)

ISACA (2017a) State of Cyber Security 2017, Part 2: Current Trends in Workforce Development (http://www.iaac.org.uk/wp-content/uploads/2018/02/2017-03-06-IAAC-cyber-profession-FINAL-Feb18-amend-1.pdf)

ISACA (2017b) State of Cyber Security 2017, Part 2: Current Trends in the Threat Landscape (https://www.cybersecobservatory.com/wp-content/uploads/2017/06/state-of-cybersecurity-2017-part-2_res_eng_0517-1.pdf)

ISACA (2018) State of Cybersecurity 2018 (https://cybersecurity.isaca.org/state-of-cybersecurity)

ISC2 (2018) Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: Cybersecurity Workforce Study 2018 (https://www.isc2.org/Research/Workforce-Study)

ISC2 (2018) Hiring and Retaining Top Cybersecurity Talent (https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx)

Joint Committee on the National Security Strategy (2018) Cyber Security Skills and the UK's Critical National Infrastructure (https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70602.htm)

Newhouse, Keith, Scribner and Witte (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. U.S. Department of Commerce (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework)

Rashid, Danezis, Chivers, Lupu, and Martin (2017) Scope for the Cyber Security Body of Knowledge (https://www.cybok.org/media/downloads/CyBOKScopeV2.pdf)

Recruitment and Employment Confederation (2017) Demand for cyber security staff to surge next year (https://www.rec.uk.com/news-and-policy/press-releases/demand-for-cyber-security-staff-to-surge-next-year-rec)

Reece and Stahl (2015) "The professionalisation of information security: Perspectives of UK practitioners", Computers & Security, 48, pp.182-195 (https://www.sciencedirect.com/science/article/pii/S0167404814001539)

Reed (2017) Innovation Through Inclusion: The Multicultural Cybersecurity Workforce (https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx)

Silensec (2017) Addressing the Cyber Security Skills Gap (https://www.silensec.com/downloads-menu/whitepapers/item/29-addressing-the-cyber-security-skills-gap)

Tech Nation (2017) The Nationality of Workers in the UK's Digital Tech Industries (http://tn2017skills.wpengine.com/wp-content/uploads/2017/12/International_Talent_report_Tech_City_UK_Nesta-2.pdf)

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

Waag and Morris (2015) Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers (http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136034/cyber-aptitude-assessment-finding-the-next-generation-of-enlisted-cyber-soldiers/)

Appendix B: quantitative questionnaire

Screener

Is this the head office for [SAMPLE S_CONAME]?

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

Hello, my name is … from Ipsos MORI, the independent research organisation. We are conducting an important survey on behalf of the UK Government Department for Digital, Culture, Media and Sport about the cyber security skills needs of all types of organisations in the UK. We are doing this survey in partnership with the University of Portsmouth. Taking part is totally confidential and anonymous for all individuals and organisations.

IF CALLING 08 NUMBER FOR CHARITY (SAMPLE S_FREENUM=1): Before I proceed, I'd like to make clear that I'm calling your 0800 number, for which you may be charged. Would you like me to proceed, or call on a different number?

As the survey focuses on cyber security skills, could I please speak to the senior person at your organisation with the most knowledge or responsibility when it comes to cyber security?

Would you be happy to take part in an interview? This should take around 15 minutes for the average organisation, and will be shorter for smaller organisations. You can withdraw from the interview at any time.

IF UNSURE WHO RELEVANT PERSON IS OR IF OUTSOURCE CYBER SECURITY: If there is no one who deals specifically with cyber security within your organisation, we would like to talk to the most senior person who deals with any IT issues. If you outsource your cyber security or IT, we would like to talk to the most senior person who makes decisions about your outsourced provider.

ADD IF NECESSARY: The survey will help the Government to understand how it can best help organisations like yours to address their cyber security skills needs. The findings will inform Government policy and the guidance offered to businesses, charities and public sector organisations.

ADD IF NECESSARY (IF OUTSOURCE CYBER SECURITY): If you outsource your IT or cyber security, the survey asks you a few questions about what services your outsourced provider covers, and how you work with them. We want to speak to you rather than the provider, so we can get the customer's viewpoint on the kind of service they provide, and the service you need.

IF UNSURE WHAT CYBER SECURITY OR CYBER SKILL IS: By cyber security, I mean any strategy, processes, practices or technologies that organisations have in place to protect their networks, computers, programs, the data they hold, or the services they provide, from unauthorised access, harm or misuse. By cyber security skills, I mean any skills your organisation thinks are necessary to carry out this cyber security role.

REASSURANCES IF NECESSARY

- The survey is for all types of businesses, charities and public sector organisations. It doesn't matter if you have not had any cyber security issues.
- The survey is not technical – we want your views, not just expert opinion on this topic.
- Findings from the survey will be published on the gov.uk website later this year, in order to help organisations like yours. We can send you a copy of the report if you wish.
- Details of the survey and our privacy notice are on the Ipsos MORI website at www.ipsos.com/ipsos-mori/en-uk/cyberskills2018.
- You can also Google the term "Ipsos MORI Cyber security skills Survey" to find the same link yourself.

- *ADD IF PUBLIC SECTOR (SAMPLE S_LEGALSTATUS=4, 5 OR 6):* To check that the survey is genuine, you can also contact DCMS.

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

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

Organisational profile

READ OUT TO ALL
First, I would just like to ask some general questions about your organisation, so I can make sure I only ask you relevant questions later on.

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

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

DUMMY VARIABLE NOT ASKED
Q1a.TYPEXDUM
Would you classify your organisation as … ?

IF TYPEX CODES 1, 2 OR DK: Private sector
IF SAMPLE S_TYPE=2 OR TYPEX CODE 3: Charity
IF TYPEX CODE 4: Public sector
(SINGLE CODE)

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

ASK ALL
Q2.SIZEA

ASK IF BUSINESS OR CHARITY (TYPEX CODES 1, 2 OR DK): Including yourself, how many employees work in your organisation across the UK as a whole?
ADD IF NECESSARY: By that I mean both full-time and part-time employees on your payroll, as well as any working proprietors or owners in the UK.
ASK IF CHARITY (TYPEXDUM CODE 2): Including yourself, how many employees, volunteers and trustees working in your organisation across the UK as a whole?
ADD IF NECESSARY: By that I mean both full-time and part-time employees on your payroll, as well as people who regularly volunteer for your organisation in the UK. This does not include operations outside the UK.
ASK IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEX CODE 4): Including yourself, how many employees and council members are there in your organisation?
ASK IF OTHER PUBLIC SECTOR (SAMPLE S_LASTATUS≠1 OR 2 AND TYPEX CODE 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

Respondent is sole trader THANK AND CLOSE *(CLOSE SURVEY)*
WRITE IN RANGE 2–99,999
(SOFT CHECK IF >9,999; ALLOW DK)

ASK IF DON'T KNOW SIZE OF ORGANISATION (SIZEA CODE DK)
Q3.SIZEB
ASK IF BUSINESS OR CHARITY (TYPEX CODES 1, 2 OR DK): Which of these best represents the number of employees working in your organisation across the UK as a whole, including yourself?
ASK IF CHARITY (TYPEXDUM CODE 2): Which of these best represents the number of employees, volunteers and trustees working in your organisation across the UK as a whole, including yourself?
ASK IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEX CODE 4): Which of these best represents the number of employees and council members in your organisation, including yourself?
ASK IF OTHER PUBLIC SECTOR (SAMPLE S_LASTATUS≠1 OR 2 AND TYPEX CODE 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

Under 10
10–49
50–249
250–999
1,000 or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

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

Under 10
10–49
50–249
250–999
1,000 or more
Don't know
(SINGLE CODE; MERGE RESPONSES FROM SIZEA AND SIZEB)

ASK IF BUSINESS OR CHARITY (TYPEX NOT CODE 4)

Q4.SALESA

In the financial year just gone, what was the approximate [turnover/income] of your organisation across the UK as a whole?

PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE £0+

(SOFT CHECK IF <£1,000 OR >£50,000,000; ALLOW DK OR REF)

ASK IF DON'T KNOW NUMERIC TURNOVER OF ORGANISATION (SALESA CODE DK OR REF)

Q5.SALESB

Which of these best represents the [turnover/income] of your organisation across the UK as a whole in the financial year just gone?

PROBE FULLY, I.E. UNTIL YOU REACH THE RIGHT RESPONSE

Less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £2 million
£2 million to less than £10 million
£10 million to less than £50 million
£50 million or more
DO NOT READ OUT: Don't know
DO NOT READ OUT: Refused
(SINGLE CODE)

DUMMY VARIABLE NOT ASKED

Q5a.SALES

Which of these best represents the [turnover/income] of your organisation across the UK as a whole in the financial year just gone?

Less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £2 million
£2 million to less than £10 million
£10 million to less than £50 million
£50 million or more
Don't know
Refused
(SINGLE CODE; MERGE RESPONSES FROM SALESA AND SALESB)

Outsourcing

ASK ALL

Q6.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 Office 365.
ADD IF NECESSARY: This may include a service provider that manages your IT or network, or helps you recover from cyber attacks.

ADD IF NECESSARY: By cyber security, I mean any strategy, processes, practices or technologies that organisations have in place to protect their networks, computers, programs, the data they hold, or the services they provide, from unauthorised access, harm or misuse.
DO NOT READ OUT

Yes
No
(SINGLE CODE; ALLOW DK)

READ OUT IF OUTSOURCE (OUTSOURCE CODE 1)
I'd now like to ask a few more questions about this outsourcing.
ADD IF NECESSARY: Just to reassure you again, all your answers are confidential. They will be grouped and analysed together with everyone else's answers to create an overall picture of the UK, rather than of your organisation alone.

ASK IF OUTSOURCE (OUTSOURCE CODE 1)
Q7.HOWMUCH
Which of these best describes your organisation?
READ OUT

We outsource **all** aspects of our cyber security
We outsource **most** aspects of our cyber security, but handle some aspects internally
We outsouce **a few** aspects of our cyber security, and handle most aspects internally
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK IF OUTSOURCE (OUTSOURCE CODE 1)
Q8.REASONOUT
What are your main reasons for outsourcing any aspects of your cyber security, instead of handling these aspects in-house?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"

Responses about not being able to manage internally
Cannot afford to recruit specialist cyber security staff
Internal staff don't have necessary skills/knowledge/experience
Too busy to manage internally
Too difficult to recruit specialist cyber security staff

Responses about added value of outsourcing
Greater expertise
Independent outlook/not biased
More up-to-date intelligence
Need constant/round-the-clock security
Quality of advice

Other responses
Already work with this outsourced provider
Comply/make it easier to comply with regulations
Contracted by parent company
Cost/more cost-effective/cheaper
Covered as part of wider contract, e.g. for IT services
Joint services provider in our building/office block

Reassuring customers/investors/stakeholders
Other *WRITE IN*
(MULTICODE OK; ALLOW DK)

ASK IF OUTSOURCE (OUTSOURCE CODE 1)
Q9.WHATOUT
Which of the following aspects of cyber security are covered by your outsourced provider or providers?
READ OUT

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. Dealing with cyber attacks
i. Any higher-level functions, which could include things like:
    - security engineering
    - penetration testing
    - using threat intelligence tools
    - forensic analysis
    - interpreting malicious code
    - or using tools to monitor user activity

Yes, outsourced
No, not outsourced
DO NOT READ OUT: Don't know
(SINGLE CODE; ASK AS A GRID; SCRIPT TO RANDOMISE STATEMENTS BUT KEEP I AND J LAST)

ASK IF OUTSOURCE HIGHER-LEVEL FUNCTIONS (WHATOUTi CODE 1)
Q10.WHATHIGHER
Which of the following specific higher-level functions are covered by your outsourced provider or providers?
READ OUT

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

Yes
No
DO NOT READ OUT: Don't know
(SINGLE CODE; ASK AS A GRID; SCRIPT TO RANDOMISE STATEMENTS BUT KEEP G LAST)

ASK IF OUTSOURCE (OUTSOURCE CODE 1)
Q11.DEALINGOUT
How confident, if at all, are you in having an informed discussion with your outsourced provider about the services they provide?
READ OUT

INTERVIEWER NOTE: IF NEVER HAD TO DO THIS BEFORE, HOW CONFIDENT WOULD THEY FEEL DOING IT IF THEY HAD TO?

Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO REVERSE SCALE)

Profile of responsible individual or team

READ OUT TO ALL
Now I'd like to ask some questions about you and others within your organisation. [IF DO NOT OUTSOURCE (OUTSOURCE NOT CODE 1): ADD IF NECESSARY: Just to reassure you again, all your answers are confidential. They will be grouped and analysed together with everyone else's answers to create an overall picture of the UK, rather than of your organisation alone.]

ASK ALL
Q12.TEAM
Within your organisation, how many people, including yourself, are directly involved in managing or running your organisation's cyber security? [IF OUTSOURCE (OUTSOURCE CODE 1): This includes whoever deals with your outsourced provider.]

WRITE IN RANGE 1–[SIZEA OR TOP END OF SIZEB] OR [99 IF SIZE=DK]
IF MICRO (SIZEA CODE<10 OR SIZEB CODE 1): (SOFT CHECK IF >3; ALLOW DK)
IF SMALL (SIZEA 9<CODE<50 OR SIZEB CODE 2): (SOFT CHECK IF >9; ALLOW DK)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF >9; ALLOW DK)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF >30; ALLOW DK)

ASK ALL
Q13.PATHWAY
ASK IF ONE PERSON (TEAM=1): How did you enter this role dealing with cyber security within your organisation?
ASK IF MORE THAN ONE PERSON (TEAM>1): Of the [TEAM] number of people directly involved in cyber security within your organisation, how many entered this role in each of the following ways?
ASK IF MORE THAN ONE PERSON (TEAM=DK): Of all the people directly involved in cyber security within your organisation, how many entered this role in each of the following ways?
READ OUT
IF ONE PERSON (TEAM=1): INTERVIEWER NOTE: CODE "1" AT RELEVANT RESPONSE

a. Recruited from a non-cyber security related previous role
b. Recruited from a previous role in cyber security
c. Absorbed this role into an existing non-cyber security related role
d. As a career starter, for example a graduate or apprentice

WRITE IN RANGE 1–TEAM OR [99 IF TEAM=DK] FOR EACH STATEMENT
(ASK AS A GRID; HARD CHECK IF TOTAL ACROSS STATEMENTS >TEAM; ALLOW DK AT EACH STATEMENT)

ASK IF ONE PERSON (TEAM=1 OR DK)
Q14.DIVERSITYA
CODE GENDER OF RESPONDENT
DO NOT READ OUT

Male
Female
(SINGLE CODE, ALLOW DK)

ASK IF MORE THAN ONE PERSON (TEAM>1)
Q15.DIVERSITYB
How many of these staff directly involved in cyber security identify as female?

WRITE IN RANGE 0–TEAM
(ALLOW DK AND REF)

DUMMY VARIABLE NOT ASKED
Q16.DIVERSITYDUM
Number of female staff working in cyber security

IF DIVERSITYA CODE 1, THEN 0
IF DIVERSITYA CODE 2, THEN 1
IF DIVERSITYA CODE DK, THEN DK
OTHERWISE RESPONSE AT DIVERSITYB

ASK ALL
Q17.QUALS
Do you [IF MORE THAN ONE (TEAM>1 OR DK): or any of the other individuals directly involved in cyber security] have, or are you working towards, any formal qualifications or certified training in any aspects of cyber security?
DO NOT READ OUT

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF QUALIFICATIONS (QUALS CODE 1)
Q18.WHICHQUALS
Which of the following types of qualifications or certified training do you [IF MORE THAN ONE (TEAM>1 OR DK): or any other team members] have, or are you working towards?
READ OUT

A specialist degree, masters or doctorate related to cyber security
A general computer science, information systems or IT degree, masters or doctorate
A cyber security apprenticeship
Any other apprenticeship
Any other technical qualifications or certified training related to cyber security
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE OK)

ASK IF OTHER QUALIFICATIONS (WHICHQUALS CODE 5)
Q19.WHICHCERT
Which other technical qualifications or certified training do you [IF MORE THAN ONE (TEAM>1 OR DK): or any other team members] have, or are you working towards?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"

Art of Hacking certification
Certified Chief Information Security Officer (CCISO)
Certified Ethical Hacker (CEH)
Certified in the Governance of Enterprise IT (CGEIT)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
Certificate in Information Security Management Principles (CISMP)
Certified Practitioner Certificate in Cloud Security
Certified Professional (CCP)
Certified in Risk and Information Systems Control (CRISC)
CyberSec First Responder
CompTIA Security+
Foundation Certificate in Cyber Security
IA Architect (certified by IISP)
IA Auditor (certified by IISP)
Information System Security Officer (ISSO, certified by IISP)
Information Security System Manager (ISSM, certified by IISP)
ISO 17024 Managing Cyber Security Risk (CCRMP)
ISO 27001 Certified ISMS
ISO 22301 Certified BCMS
IT Security Officer (ITSO, certified by IISP)
GCHQ Certified Training (GCT)
PCI DSS training
Practitioner Certificate in Information Assurance Architecture
Security & Information Risk Advisor (SIRA, certified by IISP)
Other *WRITE IN*
(MULTICODE OK; ALLOW DK)

ASK ALL
Q20.SENIORITY
As the person most in charge of cyber security within your organisation, are you … ?
READ OUT

A [director/trustee] or senior manager for the whole organisation
Someone who reports directly to the senior management team
Someone who does not report directly to the senior management team
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK ALL
Q21.FORMAL
Is cyber security a formal part of your job description, or do you cover this role informally?
DO NOT READ OUT

A formal part of their job description
Covered informally
(SINGLE CODE; ALLOW DK)

ASK ALL
Q22.COVER

I'd like you to imagine if you were away for an extended period of time, for example due to illness or annual leave. To what extent, if at all, would others in your organisation have the right skills or knowledge to cover your role with regards to cyber security?
[IF OUTSOURCE (OUTSOURCE CODE 1): ADD IF NECESSARY: This includes dealing with your outsourced provider.]
READ OUT

Completely
A great deal
A fair amount
Not very much
Not at all
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO REVERSE SCALE)

Skills and knowledge of responsible individual or team

READ OUT TO ALL
The next questions are about the current skills and knowledge of the individuals or team directly involved in cyber security. There are no right or wrong answers, and we know that not all of these skills or knowledge areas may be relevant for every organisation.

ASK ALL
Q23.RELATIVE
How important would you say it is for the [IF ONE (TEAM=1): individual/IF MORE THAN ONE (TEAM>1 OR DK): individuals or team] directly involved in cyber security within your organisation to possess each of the following? Please answer on a scale of 0 to 10, where 0 means not at all important and 10 means essential.
READ OUT

a. Soft skills, such as oral or written communication skills and team working skills
b. The skills or knowledge to deliver cyber security training
c. Understanding the legal or compliance issues affecting cyber security, such as data protection
d. Understanding how any actions or policies around cyber security can affect the organisation's performance and success
e. Basic technical skills, which could include things like:
    - setting up firewalls
    - choosing secure settings for devices or software
    - controlling who has access
    - setting up anti-virus protection
    - and keeping software up to date
f. High-level technical skills, which could include things like:
    - security engineering
    - penetration testing
    - using threat intelligence tools
    - forensic analysis
    - interpreting malicious code
    - or using tools to monitor user activity
g. Incident response skills, which could include things like writing an incident response plan, incident management and recovery from cyber security breaches

WRITE IN RANGE 0–10
(SCRIPT TO RANDOMISE STATEMENTS BUT KEEP F AND G TOGETHER; ALLOW DK)

SCRIPT TO ROTATE ORDER OF TECHNICAL, MANAGERIAL AND KNOWLEDGE

ASK ALL

Q24.TECHNICAL

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

a. Storing or transferring personal data securely, using encryption where appropriate
b. *ASK IF NOT OUTSOURCED (WHATOUTa NOT CODE 1):* Setting up firewalls with appropriate configurations
c. *ASK IF NOT OUTSOURCED (WHATOUTb NOT CODE 1):* Choosing secure settings for devices or software
d. *ASK IF NOT OUTSOURCED (WHATOUTc NOT CODE 1):* Controlling which users have IT or admin rights
e. *ASK IF NOT OUTSOURCED (WHATOUTd NOT CODE 1):* Detecting and removing malware on the organisation's devices
f. *ASK IF NOT OUTSOURCED (WHATOUTe NOT CODE 1):* Setting up software to automatically update where possible
g. *ASK IF NOT OUTSOURCED (WHATOUTf NOT CODE 1):* Restricting what software can run on the organisation's devices
h. *ASK IF NOT OUTSOURCED (WHATOUTg NOT CODE 1):* Creating back-ups of your files and data
i. *ASK IF NOT OUTSOURCED (WHATOUTh NOT CODE 1):* Dealing with a cyber security breach or attack
j. *ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEf>4 AND WHATHIGHERa NOT CODE 1):* Designing secure networks, systems and application architectures
k. *ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEf>4 AND WHATHIGHERb NOT CODE 1):* Carrying out a penetration test
l. *ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEf>4 AND WHATHIGHERc NOT CODE 1):* Using cyber threat intelligence tools or platforms
m. *ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEf>4 AND WHATHIGHERd NOT CODE 1):* Carrying out a forensic analysis of a cyber security breach
n. *ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEf>4 AND WHATHIGHERe NOT CODE 1):* Interpreting malicious code, or the results shown after running anti-virus software
o. *ASK IF HIGHER-LEVEL SKILLS MATTER AND NOT OUTSOURCED (RELATIVEf>4 AND WHATHIGHERf NOT CODE 1):* Using tools to monitor user activity

Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO RANDOMISE STATEMENTS AND REVERSE SCALE)

ASK ALL

Q25.MANAGERIAL

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

a. *ASK IF RESPONDENT NOT A SENIOR MANAGER (SENIORITY NOT CODE 1):* Communicating cyber security risks effectively to directors, trustees or senior management

b. *ASK HALF THE SAMPLE (HALF A):* Giving guidance to other staff on what an acceptably strong password is
c. *ASK HALF THE SAMPLE (HALF B):* Writing an incident response plan to deal with cyber security breaches
d. *ASK HALF THE SAMPLE (HALF A):* Carrying out a cyber security risk assessment
e. *ASK HALF THE SAMPLE (HALF B):* Carrying out a data protection impact assessment
f. *ASK HALF THE SAMPLE (HALF A):* Writing or contributing to a business continuity plan that covers cyber security
g. *ASK HALF THE SAMPLE (HALF B):* Preparing training materials or training sessions for staff who are not specialists in cyber security
h. *ASK HALF THE SAMPLE (HALF A):* Developing cyber security policies

Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO RANDOMISE STATEMENTS AND REVERSE SCALE)

ASK ALL
Q26.KNOWLEDGE
How well, if at all, would you say you [IF MORE THAN ONE (TEAM>1): or any of the other individuals directly involved in cyber security] understand each of the following?
READ OUT

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

Very well
Fairly well
Not very well
Not at all well
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO RANDOMISE STATEMENTS AND REVERSE SCALE)

Skills and knowledge of wider staff

READ OUT TO ALL
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. This includes [directors/trustees] or senior managers, [IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEX CODE 4): council members] and other core [staff/staff or volunteers] who are not specialists in cyber security.

ASK ALL
Q27.DIRECTORS
How well, if at all, would you say your organisation's [directors/trustees] or senior managers [IF LOWER-TIER LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 AND TYPEX CODE 4):, including council members,] understand each of the following?
[IF RESPONDENT A SENIOR MANAGER (SENIORITY CODE 1): ADD IF NECESSARY: If you are the only director in your organisation, please answer about your own understanding.]
READ OUT

a. The cyber security risks facing your organisation
b. *ASK IF RESPONDENT NOT A SENIOR MANAGER (SENIORITY NOT CODE 1):* Your organisation's data protection requirements
c. When cyber security breaches need to be reported externally, for example to a regulator
d. The steps that need to be taken when managing a cyber security incident
e. The staffing needs of cyber security within your organisation

Very well
Fairly well
Not very well
Not at all well
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO RANDOMISE STATEMENTS AND REVERSE SCALE)

DUMMY VARIABLE NOT ASKED
Q28.DIRECTDUM
How well, if at all, would you say your organisation's [directors/trustees] or senior managers understand each of the following?

a. The cyber security risks facing your organisation *RESPONSE FROM DIRECTORSa*
b. Your organisation's data protection requirements *IF RESPONDENT A SENIOR MANAGER (SENIORITY CODE 1), THEN RESPONSE FROM KNOWLEDGEc, OTHERWISE RESPONSE FROM DIRECTORSb*
c. When cyber security breaches need to be reported externally, for example to a regulator *RESPONSE FROM DIRECTORSc*
d. The steps that need to be taken when managing a cyber security incident *RESPONSE FROM DIRECTORSd*
e. The staffing needs of cyber security within your organisation *RESPONSE FROM DIRECTORSe*

(SINGLE CODE; ALLOW DK)

ASK ALL
Q29.CORE
How confident, if at all, would you feel in your organisation's core [staff/staff or volunteers] [IF LOCAL AUTHORITY (SAMPLE S_LASTATUS=1 OR 2 AND TYPEX CODE 4): or council members] as a whole being able to do each of the following?
READ OUT

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

Very confident
Fairly confident
Not very confident
Not at all confident
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO RANDOMISE STATEMENTS AND REVERSE SCALE)

Training and upskilling

READ OUT TO ALL
Now I'd like to ask about formal training and awareness raising activities around cyber security.

ASK ALL

Q30.NEEDS

In the last 12 months, has anyone undertaken a formal analysis of your organisation's cyber security skills or training needs?
DO NOT READ OUT

Yes
No
(SINGLE CODE; ALLOW DK)

SCRIPT TO ASK SOUGHT TO VALUE AS A LOOP FOR EACH OF THE FOLLOWING AUDIENCES:

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

ASK ALL

Q31.SOUGHT

In the last 12 months, has anyone in your organisation sought out any formal cyber security training materials or courses for [SCRIPT TO ADD LOOP TEXT]?
DO NOT READ OUT

Yes
No
(SINGLE CODE; ALLOW DK)

READ OUT IF SOUGHT TRAINING (SOUGHT CODE 1)

Now I'd like to ask a few questions about the experience of seeking out cyber security training materials or courses for [SCRIPT TO ADD LOOP TEXT].

ASK IF SOUGHT TRAINING (SOUGHT CODE 1)

Q32.BARRIERS

How much, if at all, did each of the following hinder your organisation's attempt to find training that met the needs of this group of staff? Please answer on a scale of 0 to 10, where 0 means this was not a hinderance at all, and 10 means it completely stopped you from finding training that met needs.
ADD IF NECESSARY: We are talking about [SCRIPT TO ADD LOOP TEXT].
READ OUT

a. The cost of training
b. How tailored the available training is to organisations like yours
c. How long it takes to look for relevant training
d. Not knowing what kind of training is relevant for your organisation
e. Not knowing where to find relevant training
f. Training not being in the right location or format

WRITE IN RANGE 0–10
(SCRIPT TO RANDOMISE STATEMENTS; ALLOW DK)

ASK ALL

Q33.MODE

And, regardless of whether you sought out training or not, did this group of staff undertake cyber security training in any of the following ways in the last 12 months?
ADD IF NECESSARY: We are talking about [SCRIPT TO ADD LOOP TEXT].
READ OUT

Face-to-face
Webinars
Attending cyber security seminars or conferences
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MUTLICODE OK)

ASK IF CARRIED OUT TRAINING (MODE CODES 1–3)
Q34.WORTH
How much would you say the training met the needs of this group of staff?
ADD IF NECESSARY: We are talking about [SCRIPT TO ADD LOOP TEXT].
READ OUT

Completely
A great deal
A fair amount
Not very much
Not at all
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO REVERSE SCALE)

Recruitment and retention

READ OUT TO ALL
Finally, I'd like to ask about recruitment in cyber security job roles.

ASK ALL
Q35.RECRUIT
Have you tried to recruit anyone within the last 3 or so years, i.e. since the beginning of 2015, to fill any cyber security skills needs in your organisation? This includes any current vacancies you may have.
DO NOT READ OUT

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
Q36.OTHRECRUIT
What recruitment methods have you used to find candidates for these vacancies?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"
INTERVIEWER NOTE: IF RECRUITMENT AGENCY OR WEBSITE, WERE THESE SPECIALIST AGENCIES/WEBSITES FOR CYBER SECURITY OR GENERALIST?

Recruitment agencies
Generalist recruitment agency
Specialist cyber security recruitment agency

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

Other
Asking individuals to apply directly
Headhunting (but not through recruitment agency)
Recruiting from elsewhere in organisation
Other *WRITE IN*
(MULTICODE OK; ALLOW DK)

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
Q37.VACANCIES
How many vacancies have you had in this area within the last 3 or so years?

WRITE IN RANGE 1–[SIZEA OR TOP END OF SIZEB] OR [99 IF SIZE=DK]
IF MICRO (SIZEA CODE<10 OR SIZEB CODE 1): (SOFT CHECK IF >3; ALLOW DK)
IF SMALL (SIZEA 9<CODE<50 OR SIZEB CODE 2): (SOFT CHECK IF >9; ALLOW DK)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF >9; ALLOW DK)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF >30; ALLOW DK)

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
Q38.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 of these 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

WRITE IN RANGE 0–VACANCIES OR [(SIZEA OR TOP END OF SIZEB) IF VACANCIES=DK] OR [99 IF SIZE=DK]
(ALLOW DK)

ASK IF HARD-TO-RECRUIT VACANCIES (HARD>0)
Q39.HARDREASON
IF ONE VACANCY (VACANCIES=1): What are the reasons this vacancy has been hard to fill?
IF MORE THAN ONE VACANCY (VACANCIES>1 OR DK): What are the reasons these vacancies have been hard to fill?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"

Offer not good enough
Low pay or benefits offered for post
Not offering training
Poor career progression/lack of prospects
Too much competition from other employers

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

Lack of qualifications
Lack of work experience

Other reasons
Lack of candidates generally
Remote location/poor public transport
Other *WRITE IN*
(MULTICODE OK; ALLOW DK)

Recontact

ASK ALL
Q40.RECON
This survey is part of a wider programme of research. Would you be happy to take part in a more bespoke interview with Ipsos MORI in summer 2018, to further explore some of the issues from this survey? This interview would be more of a conversation on the specific issues relevant to your organisation, rather than a structured questionnaire.
ADD IF NECESSARY: Again, the Government will not know who has taken part, either in this survey or in any follow-up interview.
ADD IF NECESSARY: The interviews would last no longer than 45 minutes and those taking part would be offered a £50 cheque or a donation to the charity of their choice.

Yes
No
(SINGLE CODE)

ASK ALL
Q41.REPORT
Would you like us to email you a PDF copy of the final report and infographics, after this research is published in late 2018? These will contain the full findings of the research, as well as findings broken down by organisation size and sector where possible.

Yes
No
(SINGLE CODE)

ASK IF WANT RECONTACT OR REPORT (RECON CODE 1 OR REPORT CODE 1)
Q42.EMAIL
IF WANT RECONTACT (RECON CODE 1): Would you be happy to give us an email address to contact you directly, so we can invite you to this follow-up interview? This email will only be used for this research, and we won't keep it after the project is finished.
IF DON'T WANT RECONTACT (RECON CODE 2): Can I please take an email address for this?

WRITE IN EMAIL IN VALIDATED FORMAT
(ALLOW REF)

CLOSE SURVEY

Appendix C: qualitative topic guide

Timings	Key questions
2–3 mins	1. Introduction ▪ Thank participant for taking part ▪ Introduce self, Ipsos MORI: independent research organisation (i.e. independent of Government), we adhere to MRS code of conduct that ensures our research is carried out in an ethical and professional manner. The code ensures research is based on voluntary informed consent and that individuals' rights, well-being and confidentiality is respected at all times. ▪ Explain the research: o We are speaking with businesses, charities and public-sector organisations to learn more about the cyber skills labour market ▪ Confidentiality: reassure all responses anonymous and that information about individuals and the company they work for will not be passed on to anyone, including back to any Government department. ▪ Get permission to digitally record ▪ Length: 45 minutes approx. ▪ Incentives: as a thank you, a £50 incentive will be paid to the participant or a charity of their choice.
2–3 mins	2. Context *This section aims to warm up the participant and gain some general information about their role in the organisation.* ▪ Could you briefly give an outline of what your organisation does and what its main purpose is? ▪ What is your role within the organisation? o How long have you been with the organisation? o What are your day-to-day tasks? Prompt on cyber security responsibilities. o How much of your role relies on broad cyber security-related skills, such as project management, and how much of it relates to specifically technical skills? o Who makes decisions around cyber security/cyber security training and recruitment within your organisation? o And does your organisation outsource any aspects of its cyber security? [Researcher: Note answer to see if respondent is eligible for section 4]
5–7 mins	3. Perception of cyber skills *This section explores the participant's perceptions of what cyber skills are and how they impact upon their organisation.* ▪ What do you define as a cyber skill? o What kind of technical skills do you think would fall under the umbrella of cyber skills?

	▪ Prompt businesses: Information security, Business continuity, physical security, incident response and IT service continuity. ▪ Prompt public sector organisations: Governance and risk, penetration testing, system architecture and forensics? o How do you differentiate these from broader IT skills? o What kind of soft skills fall under the umbrella of cyber security? Why do these matter/what difference do they make? ▪ How would you define and differentiate technical and non-technical cyber skills? ▪ Are there any professional cyber security roles in your organisation? Are there any roles that involve cyber security but labelled as something else? ▪ Is cyber security viewed as an important issue within your organisation? Prompt on whether it is seen as an important issue by senior management / directors / trustees. ▪ Do you feel your organisation has adequate cyber security provisions? Prompt on why they feel it is adequate/inadequate. o 'If adequate' What makes you think what you do is adequate? ▪ Is there someone with high-level technical skills, such as penetration testing, in the organisation? o If 'inadequate', what do you feel are the barriers to attaining good levels of cyber security? Explore around; Cost - perceived as unimportant – lack the capacity – difficulty outsourcing. Are there specific skills which are especially in-demand but in short supply? This could include soft or technical skills such as cryptography, penetration testing, incident management, etc.
5–8 mins	<u>5. Recruitment and supply of skills</u> *This section explores organisations practices around recruiting for cyber security roles and the available supply of skills in the market.* ▪ Is your organisation looking to recruit to fill any cyber security professionals? o If no, why? Prompt around whether they feel they need to. ▪ What are the career backgrounds of the individuals with cyber security responsibility in your organisation? What was their career route into cyber security? ▪ Which cyber skill-sets is your organisation looking to acquire? Are there any specific cyber security/technical skills in particular? ▪ Do you think a cyber security professional includes technical and non-technical skills. What would you see as the weighting of technical/non-technical skills in these roles? ▪ Does your organisation look for formal qualifications when recruiting cyber security related positions (either for recruitment to technical or non-technical roles)? o If yes, what do you consider to be formal qualifications? What specific qualification would you look for? ▪ How important do you consider formal qualification to be for cyber security professional? Why? o If no, why not? How do you assess whether someone has the necessary skills and expertise to carry out their job effectively? Are there non-cyber security related qualifications which provide sufficient or equivalent assurance of skills?

	○ Do you consider practical knowledge and soft skills as valuable as a formal qualification? ▪ What channels are you using to recruit such roles? How hard is it to acquire the appropriate cyber skills to meet the needs of your organisation? What difficulties or barriers have you encountered when recruiting for cyber security roles? ▪ What actions have you taken to assess what skills your organisation is in need of? If no actions, why? ▪ Do you feel there is adequate supply of individuals with the relevant cyber skills to meet the needs of your organisation? ○ Do you find there are sufficient professionals available with cyber-security as a secondary skill? ○ Differentiate between entry level cyber security roles and more senior cyber security management roles. ▪ What level of experience do you typically look for when recruiting cyber professionals? ▪ If looking for experienced individuals (5-10 years experience) do they feel they have to pay extra to recruit these people? What is discouraging them from recruiting those with less experience? ▪ In your experience, where have experienced cyber-security professionals developed their initial experience? ○ Are there any particular skills that are lacking in the market and supply is not meeting demand? ▪ Do you take any steps to encourage diversity when recruiting cyber security staff? Do you look for people from specific backgrounds when recruiting for cyber-security roles? ○ Are there people from specific-backgrounds which you have found especially well-suited to cyber-security roles? Especially with regards to people moving sideways into the cyber security profession? ▪ Do you think your organisation will need more cyber security expertise in the future? ▪ Does your organisation host any apprenticeships? Would you consider a cyber security apprenticeship? if not, why?
10–12 mins	<u>6. Training and upskilling</u> *This section explores views on training and upskilling around cyber skills whether the training resources available meet the demands of organisations.* ▪ What are your organisations training and upskilling needs with regards to cyber security? ○ Differentiate between the requirement for directors/senior management, cyber staff and core staff, technical and non-technical roles. Probe throughout section. ○ Differentiate between technical and non-technical skills and how training/upskilling differs between them. Probe throughout section. ▪ What training products or services has your organisation accessed? If none, why have they not accessed any? ○ For each training product or service accessed, how effective were these as a solution to your training needs? ○ How could the training you used be improved?

	▪ Who has accessed training in the organisation (is it core staff or cyber-security professionals only) and at what level? Are needs being met at every level, or some but not others? ▪ Can you tell me about the process in selecting a training product or service? o How did you reach the decision? o Was it difficult to locate appropriate products or services? ▪ Does the training available in the market meet the needs of your organisation? ▪ Do you feel your organisation has experienced tangible benefits from carrying out cyber security training? If so, what are they? ▪ Do you feel your organisations sees value in paying for training on cyber security? Probe, does your organisation allow sufficient time for cyber security training. ▪ Is there any concern that upskilling your cyber security team may cause difficulty in retaining these staff once they are more skilled? o If yes: Would you be willing to give training if it was cheaper or higher quality, or are you more concerned about retention? ▪ How challenging is it to keep up with changes in cyber security? Prompt specifically on how training and upskilling fit in here. o Prompt: what actions (if any) do they take to keep up-to-date with training and upskilling products?
5–7 mins	<u>7. Key recommendations</u> *This section looks at what recommendations organisations have for improving the cyber skills labour market and specific recommendations for government and industry.* ▪ How could it be made easier for your organisation to train or upskill existing staff, or recruit new staff to fill cyber skill gaps? ▪ Are you aware of any government interventions taking place? Do you think these are successful? o What more do you think government can do to help you meet your cyber skills needs? Probe for specific recommendations. o Are you aware of the Cyber Skills Immediate Impact Fund? If no, EXPLAIN This is a fund open to organisations, such as training providers and charities, to service a range of employers and address the cyber skills shortage in the UK. For example, funds could be used for training costs, project staff costs, equipment, job fairs and marketing campaigns. ▪ What do you think industry can do to help you meet your cyber skills needs? ▪ Do you have any recommendations for how the cyber skills labour market could be improved to meet the needs of your organisation?
2–3 mins	<u>8. Summary and close</u> ▪ Is there anything that we haven't discussed that you would like to raise? ▪ Overall, what do you think is the one thing I should take away from the discussion today? ▪ Reassure about confidentiality, THANK AND CLOSE

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

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

About Ipsos MORI's Social Research Institute

The Social Research Institute 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. This, combined with our methods and communications expertise, helps ensure that our research makes a difference for decision makers and communities.