Cyber security skills in the UK labour market 2020

Technical report

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

Department for
Digital, Culture,
Media & Sport

Ipsos MORI

Contents

1 Overview

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

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 Full research objectives

The research aimed to gather evidence on:

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

It also aims to create a set of recommendations on what the government and industry can do to tackle the cyber security skills gap.

1.2 Summary of methodology

The methodology consisted of 6 strands. The role of the first 2 strands was mainly to feed into the development of the quantitative survey (strand 3) and qualitative research (strand 4), by scoping out the gaps in the existing literature and the topics that should be explored.

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

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

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

3. **Quantitative surveys** – Ipsos MORI conducted representative telephone surveys with 4 audiences: general businesses, public sector organisations, charities and cyber sector firms. These surveys gathered the main estimates on skills gaps and shortages reported in this study. Fieldwork was between 7 August and 8 October 2019.

4. **Qualitative interviews –** Ipsos MORI conducted a more focused strand of qualitative research, with in-depth interviews split across large organisations and cyber sector firms. The interviews explored the challenges these organisations faced in addressing skills gaps and shortages, and the approaches they were taking on recruitment, training, outsourcing and workplace diversity. Interviews took place across September 2019.

5. **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Burning Glass Technologies labour market database, showing the number, type and location of vacancies across the UK. This also covers remuneration, descriptions of job roles and the skills, qualifications and experience being sought by employers. This work covered vacancies over a period of 3 years, from September 2016 to the end of August 2019.

6. **Recommendations workshop** – Ipsos MORI carried out a workshop with key stakeholders from government, industry and academia to discuss the findings from the preceding strands and contribute to the project's recommendations. This took place in November 2019.

1.3 Similarities and differences from the 2018 study

The 2018 study consisted of:

- A rapid evidence review of existing research on cyber skills and skills gaps
- Scoping interviews with industry experts, across trade associations, multinational businesses, cyber security specialists, training providers, recruitment agencies, academics and government
- Quantitative surveys with businesses, public sector organisations and charities
- Follow-up qualitative interviews with a mix of organisations that took part in the survey

The methodology for the quantitative surveys across both years is the same and the survey findings are intended to be comparable, where the same questions have been asked to the same groups.

However, there are various differences in the methodology this year:

- There were no scoping interviews this year. In 2018, these interviews mainly informed the questionnaire development and the definition of cyber security skills. Coming up with a definition was a specific objective of the 2018 study. This time, we already had a baseline questionnaire to adapt and there was no longer an objective to define cyber security skills

- Strands 2 (training provider market scoping), 5 (job vacancies analysis) and 6 (recommendations workshop) are entirely new for this year. These new strands allowed us to more effectively address the research objectives around training provision, recruitment and study recommendations

- In the quantitative survey, cyber sector firms were included as a sampled group for the first time this year. This was not possible in 2018 because there was no robust sample frame for these firms. This year's fieldwork came after DCMS's Cyber Sectoral Analysis 2020,[3] which created a database of UK cyber sector firms. The findings from this sample form a baseline for future studies. We have

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

also, in our main report, included findings from a separate, comparable survey of the same group (using the exact same sample frame and survey methodology) carried out as part of the Cyber Sectoral Analysis 2020. Fieldwork for this survey was carried out in summer 2019

In addition, in the quantitative survey, the sample size for charities is lower this year (201) than in 2018 (470). The margins of error for the charity findings this year are consequently higher. They were ±4-6 percentage points (accounting for weighting) in 2018 and are ±6-10 percentage points this year. The balance of the interviews this year reflected DCMS's priorities across all the sampled groups. It also made it feasible to include cyber sector firms this year within the total 1,558 quantitative survey interviews conducted

- The questionnaire for the quantitative surveys was revised with different routes for the general audience (businesses, public sector organisations and charities) and cyber sector firms. The main implications for the results were that, this year, the general audience surveys included new questions on job titles and descriptions, and only the cyber sector survey included questions on diversity, qualifications and recruitment. This followed the recommendations from the strand 1 methods review, which noted that questions on diversity, qualifications and recruitment were either answered by too few respondents or not understood well enough by the general business audience in 2018 to be useful

- The quantitative survey questionnaire was not cognitively tested again this year, having already been thoroughly tested in 2018

- The fieldwork for the quantitative survey shifted from summer in 2018 to autumn in this latest survey

- The qualitative strand focused on a different audience this year. In 2018, it followed up a range of organisations that took part in the quantitative survey, of all sizes and sectors. This year, we focused on large organisations and cyber sector firms, to better address objectives around recruitment, training, diversity and outsourcing. The small and medium-sized organisations we interviewed in 2018 typically had more basic skills needs, so could not discuss many of these more advanced skills issues. DCMS provided the sample of large organisations, including specific sectors with significant physical and digital infrastructure challenges such as finance, energy and transport organisations

1.4 Differences from other well-known studies looking at cyber security skills

A note on the UK cyber security workforce size estimate from the 2019 Cybersecurity Workforce Study

ISC2 is a global membership organisation for cyber security professionals. It publishes an annual Cybersecurity Workforce Study, the most recent of which was published in November 2019.[4] This is a study of the global cyber security workforce and largely reports its findings at a global level.

The 2019 ISC2 report includes one specific estimate for the UK, suggesting there are c.289,000 individuals in the UK cyber security workforce. It is not possible for us to validate their estimate with our data, given the vast differences in methodologies between our 2 studies (outlined later in this section) and a lack of published technical information on the UK sample size and representativeness of the ISC2 data. The estimate is also likely to have a substantive margin of error around it.

[4] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study#. Before 2018, these were known as the Global Information Security Workforce Studies, or GISWS.

There are 2 sets of DCMS data that do provide an insight on the size of the UK cyber security workforce:

- DCMS's Cyber Sectoral Analysis 2020[3] estimates 42,855 full-time employees working in cyber roles in the UK cyber sector, across the 1,221 cyber security companies that make up this sector. This excludes individuals working in cyber roles outside of these companies

- In this cyber security skills research, we estimate that there were 393,257 unique job postings for cyber security roles in the past 3 years (see Chapter 6 of the main report). This suggests that the ISC2 figure of c289,000 may be an underestimate, although we cannot say this for sure. Not all of these job postings will have been filled, and some may be to replace individuals who have left the job (so would be double-counting people in the workforce)

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

The findings from the ISC2 2019 report touch on similar themes to our study (such as skills gaps, career pathways and qualifications) but they are not directly comparable. This is also the case for other well-known surveys that have been published since the previous DCMS cyber security skills study, including the EY Global Information Security Survey 2018-19[5] and the ISACA State of Cybersecurity 2019[6].

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

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

- This research measures skills gaps – the number of organisations lacking specific cyber security skills – in a particular way. As we cannot objectively test whether organisations are capable of carrying out specific cyber security tasks involving specialist skills, we instead ask about their confidence at being able to carry out a range of these tasks (see Chapter 4 of the main report for full details). This continues the methodology we established in the 2018 study

[5] See https://www.ey.com/en_gl/giss.
[6] See https://www.isaca.org/info/state-of-cybersecurity-2019/index.html.

1.5 Acknowledgements

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

- Sam Donaldson, Perspective Economics
- Professor Mark Button, Institute for Criminal Justice Studies, University of Portsmouth
- David Crozier, Centre for Secure Information Technologies, Queen's University Belfast
- Professor Steven Furnell, University of Plymouth
- Professor Andrew Martin, University of Oxford
- Dr Victoria Wang, Institute for Criminal Justice Studies, University of Portsmouth

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

2 Methodology and evidence review

This strand took place across June and July 2019. It had 3 parts:

1. Professor Steven Furnell of the University of Plymouth carried out a literature review of cyber skills and skills gaps. This was intended to update the same kind of review we undertook in the 2018 study, so focused mainly on new researched published since October 2018 (with occasional references to earlier studies that were not fully reviewed in 2018).

   Professor Furnell and the wider research team (Ipsos MORI, Perspective Economics, David Crozier, Professor Mark Button, Dr Victoria Wang and Professor Andrew Martin) compiled a longlist of 47 sources for inclusion. DCMS approved this list and flagged the priority documents for inclusion. The review focused mainly on 18 core documents, again approved by DCMS, with brief references to various other pieces. This removed documents that were less relevant or had unclear methodologies.

2. Professor Furnell also wrote up case studies of other nations' approaches to tackling cyber skills gaps, based on a further 20 documents gathered via the wider research team and DCMS. This focused on pulling out the key details of cyber security skills strategies and programmes in other countries.

3. Ipsos MORI carried out a review of the 2018 questionnaire, highlighting questions that filtered through to very small samples or received a high "don't know" response in the previous study. We also asked the academic partners to comment on the questionnaire and suggest new question areas and improvements. The changes to the questionnaire are covered in Chapter 4 rather than here.

All 3 parts informed the approach for the primary research – particularly the questionnaire development in the quantitative survey.

Professor Furnell's output for parts 1 and 2 is reproduced in full in Appendix A.

3 Training provider market scoping

This strand took place between June and August 2019 and was led by Perspective Economics, with support from Ipsos MORI. This was an entirely new strand of research, not conducted in 2018. The intentions were to:

- Better address the research objective around the types of training products and services available, and whether these are meeting industry needs
- Categorise training provision in a way that could be explored in strands 3 and 4

The primary research findings from this strand have been summarised in the main report.

3.1 Training provider interviews

Perspective Economics and Ipsos MORI conducted 7 in-depth interviews among cyber security training providers. These were all identified from the DCMS database of cyber sector firms built during the Cyber Sectoral Analysis 2020.[7] Perspective Economics recruited these organisations via direct email and telephone contact. We included an incentive of £50 (either going to participants or to charity) to encourage participation.

The interviews explored:

- The types and areas of training currently offered
- The types and areas of training most in demand and the direction of travel for the next 2-5 years
- The kinds of clients demanding training and their awareness of their training needs
- The demand for and role of qualifications and certification in training
- The scalability of training
- Partnerships with industry and academic institutions
- Involvement in (and experience of) government-backed cyber security skills programmes

To help with the final area, recruitment focused on training providers involved in the Cyber Skills Immediate Impact Fund (CSIIF).[8] In total, 6 of the 7 providers we interviewed were involved in the CSIIF.

The topic guide for this part is in Appendix B.

3.2 Review of all UK training provider websites

This strand also included a secondary research component. Perspective Economics carried out systematic web scraping of UK training provider websites to establish what products and services they offer and give an overview of the market. We used the findings to create a categorisation of training products and services (reproduced in Appendix C). Ipsos MORI cross-referenced this categorisation against the quantitative survey questionnaire to ensure we collected the right information.

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

[8] See https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund.

4 Quantitative surveys

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

4.1 Questionnaire development

Ipsos MORI developed the questionnaire and all the other survey instruments (such as the interviewer briefing notes, a reassurance email for respondents and a survey website page). The starting point for this work was the 2018 questionnaire.

The strand 1 questionnaire review and strand 2 training provider scoping informed the changes made to this year's questionnaire. The DCMS team and the National Cyber Security Centre (NCSC) also reviewed the questionnaire, particularly the section measuring skills gaps. Their contribution covered both basic and advantaged skill areas. The main changes were as follows:

- We shortened the questionnaire introduction to making it quicker and easier for interviewers.
- We added a new job title and department profiling question for the general audience (businesses, public sector organisations and charities) to better understand where cyber security responsibilities sat within organisations and whether these were labelled as cyber roles (addressing a specific research objective)
- We restricted the following questionnaire sections to cyber sector firms only: diversity, qualifications and recruitment. This followed the recommendations from the strand 1 methods review, which noted that these questions were either answered by too few respondents or not well understood by the general audience in 2018 to be useful
- We substantively overhauled the training section based on academic feedback. The new questions cover how well organisations think they understand their training needs, whether this is backed up by a formal analysis of training needs, which groups receive training, and the content and nature of this training (e.g. internal or external, mandatory or non-mandatory and graduate or non-graduate training)

Any new questions were typically added at the end of the relevant questionnaire section. This helped to avoid order effects which would limit the validity of trend data.

Many of the cyber sector firms interviewed for this study had also taken part in the earlier DCMS survey carried out in summer 2019, as part of the Cyber Sectoral Analysis 2020.[9] To avoid asking these firms to repeat the same information in this latest survey, the survey script included a question that collected permission for us to reuse the data from the earlier survey, thereby filtering this sample out of several firmographic questions (on the size of their total workforce and their cyber workforce specifically).

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

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

4.2 Sampling

The target population included:

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

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

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

The sample frame for businesses and public sector organisations was the government's Inter-Departmental Business Register (IDBR), which covers businesses in all sectors, including the public sector, across the UK at the enterprise level. This is the main sample frame for government surveys of businesses and for public sector organisations. Organisations in the agriculture, forestry and fishing sectors (SIC, 2007 category A) were excluded. DCMS 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 2018 study.

In total, we selected 48,702 businesses and public sector organisations from the IDBR. This year we selected more leads than in 2018 (when it was 37,871) because in our more recent experience of the IDBR we found that there were far fewer IDBR leads that had telephone numbers than in previous years.

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

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

Table 4.1 breaks down the originally selected sample by size and sector. As the survey outcomes later in this chapter show, only 9,966 IDBR leads were included in the final survey, with the rest being unusable (i.e. with no telephone number) or being held in reserve.

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

Table 4.1: Pre-cleaning selected IDBR 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)	1,393	102	181	1,676
F	Construction	3,939	52	69	4,060
G	Retail or wholesale (including vehicle sales and repairs)	2,433	108	410	2,951
H	Transport or storage	5,255	185	176	5,616
I	Food or hospitality	2,101	99	97	2,297
J	Information or communications	10,077	144	253	10,474
K	Finance or insurance	1000	240	128	1,368
L, N	Administration or real estate	3,924	110	224	4,258
M	Professional, scientific or technical	5,807	95	232	6,134
O	Other public sector	76	199	113	388
P	Education (including academies)	3,396	122	70	3,588
Q	Health, social care or social work (including NHS)	4,133	140	47	4,320
R, S	Entertainment, service or membership organisations	1,468	54	50	1,572
	Total	45,002	1,650	2,050	48,702

Charity sample frames and sample selection

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

- The Charity Commission for England and Wales database: 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 2018 study.

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

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

As discussed in Chapter 1, the number of charity interviews was reduced this year to 201 (from 470 last year). The sample was proportionately stratified by country and disproportionately stratified by income band. This stratification reflects the fact that the variance in survey responses tends to be higher among larger (high-income) charities and because it would still allow some basic subgroup analysis by income band, despite the lower sample size.

As the entirety of the 3 charity regulator databases were used for sample selection, there was no restriction in the amount of charity sample that could be used, so no equivalent to Table 4.1 is shown for charities. In total, we sampled 562 charities to achieve 201 interviews.

Cyber sector sample frame and sample selection

For cyber sector firms, we used the DCMS sector database that was created as part of the Cyber Sectoral Analysis 2019 (also carried out by Ipsos MORI and Perspective Economics). Perspective Economics built this sample frame, a list of 1,221 UK cyber sector firms, from the Orbis and Beauhurst databases. From this database, there were 904 records with telephone numbers.

All 904 leads were included in the survey. In other words, this survey was carried out using a census approach and achieved a simple random sample of 205 interviews.

Sample telephone tracing and cleaning (required for IDBR and Scottish charity samples)

Not all the original sample was usable. In total, 42,426 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 DBS Data[11] (matching to both their business and, for micro businesses and charities, residential number databases) to fill in the gaps where possible. This increases the amount of usable sample and helps to reduce the likelihood of non-response bias affecting the survey. There was already very high telephone coverage for charities from England and Wales (92% with telephone numbers), and Northern Ireland (100% with telephone numbers), which provided more than enough usable sample and already minimised the possibility of non-response bias. Therefore, as per the previous study, 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 phrase “parish council”, “town council” or “community council” to highlight further leads for removal.

Following telephone tracing and cleaning, the usable business sample amounted to 11,731 leads (i.e. 24% of the original sample frame). The composition of this sample is shown in Table 4.2. For the Scotland charities sample, 2,786 leads out of the original sample frame of 24,680 leads (11%) had telephone numbers after matching.

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

Table 4.2: Post-cleaning available IDBR 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)	602	97	165	864
F	Construction	768	47	62	877
G	Retail or wholesale (including vehicle sales and repairs)	762	100	370	1,232
H	Transport or storage	642	175	155	972
I	Food or hospitality	431	78	86	595
J	Information or communications	1,112	115	211	1,438
K	Finance or insurance	626	215	110	951
L, N	Administration or real estate	629	87	205	921
M	Professional, scientific or technical	911	86	197	1,194
O	Other public sector	19	168	99	286
P	Education (including academies)	819	106	69	994
Q	Health, social care or social work (including NHS)	795	125	41	961
R, S	Entertainment, service or membership organisations	357	45	44	446
	Total	8,473	1,444	1,814	11,731

The usable leads for the survey were randomly allocated into separate batches for businesses and charities. Each batch included leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band, from 2018 and from previous batches. In other words, we selected more sample in sectors and size bands where there was a higher target, or where response rates were expected to be relatively low.

We drew up and released subsequent batches of sample as and when the live sample was exhausted. Not all available leads were released in the main stage (see Tables 4.3, 4.4 and 4.5 for the total sample loaded).

The cyber sector sample did not require further telephone tracing or cleaning. This process had already been carried out in the previous survey conducted in summer 2019, as part of DCMS's Cyber Sectoral Analysis 2020.

4.3 Piloting

Cognitive testing was required in 2018 when the questionnaire was developed from scratch. This year, much of the questionnaire remained unchanged or involved rerouting existing questions to the new cyber sector group. Therefore, cognitive testing was not required.

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

We carried out 54 live pilot telephone interviews between 7 and 8 August, among the 4 audiences for the study (general businesses and public sector, charities and cyber sector firms).

Following the pilot, we made 2 minor sets of changes to the questionnaire:

- We added subheadings to the TITLE question to making coding of responses quicker for interviewers. We also added various codes to this question based on the “other” responses from the pilot
- We added new reassurances around confidentiality alongside the diversity questions

These 54 interviews were included in the final dataset, as the changes we made were not substantive enough to affect the comparability of findings before and after the pilot in any way.

4.4 Fieldwork

All survey fieldwork (including the live pilot) was carried out from 7 August to 8 October 2019 using a Computer-Assisted Telephone Interviewing (CATI) script.

In total, we completed 1,558 telephone interviews, comprising:

- 1,046 businesses (excluding agriculture, forestry and fishing businesses)
- 106 public sector organisations (excluding parish councils)
- 201 registered charities
- 205 cyber sector firms

The average interview length was c.15 minutes for businesses and public sector, c.16 minutes for charities and c.13 minutes for cyber sector firms.

Fieldwork preparation

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

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

Screening of respondents

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

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

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

When an interviewer established that the organisation was eligible, and that this was the head office, we asked them to identify the senior member of staff who has the most knowledge or responsibility when it comes to cyber security.

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

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

Random-probability approach and maximising participation

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

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

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

Several steps were taken to maximise participation in the survey and reduce non-response bias, beyond the general management and scheduling of the fieldwork and interviewing team to produce the best results. Interviewers could send a reassurance email to prospective participants to confirm the legitimacy of the study and provide more information. We also had a study website and GOV.UK page to reassure respondents that this was a bona fide government survey. Finally, we offered respondents a copy of the report and a government cyber security help card (reproduced in Appendix E) to encourage participation.

Fieldwork monitoring

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

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 4.3 shows the final outcomes and the adjusted response rate calculation for business and public sector (the IDBR sample). Tables 4.4 and 4.5 shows the equivalent for charities and cyber sector firms.

Compared to 2018, the unadjusted response rate for the IDBR sample is slightly lower (11% this year, vs. 14% in 2018). For charities, it is higher (36% vs. 30%). The lower rate for businesses is potentially down to various issues, including a change in the fieldwork period from summer in 2018 to autumn in this latest survey, increasing awareness of cyber security potentially making businesses more reticent to take part and a more general decline in business survey response rates (regardless of the topic).

Table 4.3: Fieldwork outcomes and response rate calculations for businesses and public organisations (IDBR sample)

Outcome	Total
Total sample released	9,966
Completed interviews	1,152
Incomplete interviews	51
Ineligible leads – established during screener[12]	315
Ineligible leads – established pre-screener	84
Refusals	1,314
Unusable leads with working numbers[13]	1,160
Unusable numbers[14]	1,078
Working numbers with unknown eligibility[15]	4,812
Expected eligibility of screened respondents[16]	79%
Expected eligibility of working numbers[17]	55%
Unadjusted response rate	11%
Adjusted response rate	24%

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

Table 4.4: Fieldwork outcomes and response rate calculations for charities

Outcome	Total
Total sample released	562
Completed interviews	201
Incomplete interviews	5
Ineligible leads – established during screener	9
Ineligible leads – established pre-screener	10
Refusals	69
Unusable leads with working numbers	59
Unusable numbers	15
Working numbers with unknown eligibility	194
Expected eligibility of screened respondents	92%
Expected eligibility of working numbers	77%
Unadjusted response rate	36%
Adjusted response rate	48%

Table 4.5: Fieldwork outcomes and response rate calculations for cyber sector firms

Outcome	Total
Total sample released	904
Completed interviews	205
Incomplete interviews	6
Ineligible leads – established during screener	0
Ineligible leads – established pre-screener	6
Refusals	176
Unusable leads with working numbers	122
Unusable numbers	26
Working numbers with unknown eligibility	363
Expected eligibility of screened respondents	100%
Expected eligibility of working numbers	75%
Unadjusted response rate	22%
Adjusted response rate	31%

4.5 Data processing and weighting

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

The IDBR contains businesses that might also be registered charities. Moreover, the public sector organisations within the IDBR sample are split across several sectors (most commonly SIC 2007 sectors P, Q and O[18]), so cannot be fully identified at the sampling stage. We allowed all IDBR-sampled

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

organisations to self-identify as either a private sector organisation, public sector organisation or charity in the interview. We then took this as their designated status in the final data.

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

Coding

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

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 2018 survey and has been tested and validated in previous surveys, such as DCMS's Cyber Security Breaches Survey series.[19] The sector groupings used in the main report match those shown in Tables 4.1 and 4.2.

Weighting

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

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

We used 4 separate weighting schemes:

1. For businesses, there were non-interlocking weights by size and sector, based on the population profile in the 2018 Department for Business, Energy and Industrial Strategy (BEIS) business population estimates (the latest ones published at the time of data processing).[20] Non-interlocking weighting means that we did not weight by size *within* each sector, but weighted the whole sample separately by size and then by sector. Interlocking weighting (i.e. weighting by size band within each sector) was also possible but would have potentially resulted in very large weights. This would have reduced the statistical power of the survey results without making any considerable difference to the weighted percentage scores for each question, so was not applied.

   Very shortly after completing the data processing for this survey, BEIS published the 2019 estimates. While the 2019 estimates highlight an increase in the total number of businesses (an increase of 3.5% since 2018), we expected that this would have a negligible impact on the data, so have kept the weighting to match the 2018 estimates in the final data.

[19] See https://www.gov.uk/government/collections/cyber-security-breaches-survey.
[20] See https://www.gov.uk/government/statistics/business-population-estimates-2018.

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

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

3. For public sector organisations, we also weighted based on the public sector profile in the 2018 BEIS business population estimates.

4. One complexity in the weighting of private and public sector organisations is that certain sectors of the economy contain a mix of the private and public sector – especially education (SIC sector P) and health (SIC sector Q). For analysing these 2 sector subgroups, we created a fourth weighting scheme that merged the private and public sector population profiles from the 2018 BEIS estimates.

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

- There was no disproportionate sampling for this survey sample, so corrective weights were not needed

- We compared the profile by size band achieved in this survey to the profile from the earlier Cyber Sectoral Analysis 2020 survey,[21] which was also not weighted. This is the best comparison to indicate whether the sample is skewed in any way. Both surveys broadly achieved the same profile

- There is no other reliable profile data on the sector, beyond the estimates from the Cyber Sectoral Analysis 2020 survey

Tables 4.6 to 4.8 show the unweighted and weighted profiles of the data.

Table 4.6: Unweighted and weighted sample profiles for businesses (excluding industry sectors that contain both private and public sector organisations)

	Unweighted %	Weighted %
Size		
Micro or small (1–49 staff)	78%	97%
Medium (49–249 staff)	13%	3%
Large (250+ staff)	9%	1%
Sector		
Administration or real estate	8%	13%
Construction	7%	13%
Entertainment, service or membership organisations	2%	7%
Finance or insurance	8%	2%
Food or hospitality	5%	10%
Information or communications	11%	6%
Professional, scientific or technical	10%	15%

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

	Unweighted %	Weighted %
Retail or wholesale	12%	18%
Transport or storage	9%	4%
Utilities or production (including manufacturing)	11%	7%
Region		
East Midlands	7%	7%
Eastern	10%	10%
London	15%	12%
North East	2%	2%
North West	10%	9%
Northern Ireland	4%	5%
Scotland	8%	10%
South East	16%	16%
South West	9%	10%
Wales	4%	4%
West Midlands	8%	9%
Yorkshire and Humberside	7%	8%

Table 4.7: Unweighted and weighted sample profiles for charities

	Unweighted %	Weighted %
Income band		
£0 to under £100,000	30%	69%
£100,000 to under £500,000	19%	12%
£500,000 or more	40%	6%

Table 4.8: 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)	27%	1%
Medium (49–249 staff)	44%	26%
Large (250+ staff)	28%	73%
Sector		
Education (including academies)	10%	2%
Health, social care or social work (including NHS)	8%	5%

5 Qualitative interviews

Concurrently with the survey, Ipsos MORI conducted 23 qualitative in-depth interviews in September 2019. This included 15 large organisations and 8 cyber sector firms. The balance of interviews towards large organisations reflects the fact that the quantitative survey estimates would be less reflective of these types of very large organisations. Because it was not feasible to cover them substantively in the survey, it became more important to cover a wide range of these organisations in this qualitative strand.

5.1 Sampling and recruitment

DCMS provided Ipsos MORI with a list of high-priority large organisations to contact for this strand. DCMS had notified these organisations of the research beforehand and encouraged them to take part. These organisations had not taken part in the quantitative survey. Given the small sample size, we informed all large organisations taking part that there was a small chance that DCMS would be able to identify them based on the research findings, even though we would exclude any names of organisations or individuals in the reporting – all organisations we spoke to were happy to take part on this basis.

The cyber sector sample was based on a recontact question from the quantitative survey, sampled at 2 points during fieldwork.

Ipsos MORI recruited all the interviews by email and telephone. Our specialist business recruiter recruited from both the DCMS sample and the recontact sample built up during survey fieldwork. We offered a £50 charity donation incentive to each participant to encourage participation.

5.2 Fieldwork

Each interview was carried out by telephone by one of the Ipsos MORI core research team and lasted c.45-60 minutes.

The topics for discussion were compiled collaboratively between Ipsos MORI and DCMS. The starting point was a list of topics identified as evidence gaps by Professor Furnell in the literature review. Further to this, Ipsos MORI and DCMS also discussed the research topics that would better suit a qualitative approach during the development of the quantitative questionnaire.

The interviews explored the challenges these organisations faced in addressing skills gaps and shortages, and the approaches they were taking on recruitment, training, outsourcing and workplace diversity.

The full topic guides for large organisations and cyber sector businesses are contained in Appendix F.

5.3 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 one of these discussions. At the end of fieldwork, we drew out key themes and case studies to include in the final findings.

6 Job vacancies analysis

Perspective Economics led this strand of the research. While it was carried out concurrently with the quantitative survey, the job data included in the analysis stretches from September 2016 to the end of August 2019, i.e. 3 years of data.

6.1 Methodology

The Burning Glass Technologies definition of cyber job roles

Burning Glass Technologies[22] has been tracking the cyber security job market since 2013. Its database has a basic filter for cyber security job postings based on job titles, required skillsets and certifications. This filter broadly covers, but does not distinguish between, roles that Burning Glass Technologies defines as “core” and “cyber-enabled”. The difference between the two, adapted from the Burning Glass Technologies definition[23], is as follows:

- Core cyber roles are formally labelled or commonly recognised as cyber security jobs. They have a greater demand for skillsets and tools directly related to cyber security, such as information systems, cryptography, information assurance, network scanners, and security operations. In other words, these are job roles where some aspect of cyber security is the main job function. This would typically include job titles such as Cyber Security Architect, Cyber Security Engineer, Cyber Security Consultant, Security Operations Centre (SOC) Analyst and Penetration Tester

- Cyber-enabled roles are not formally labelled or commonly recognised as cyber security jobs but require cyber security skills. Alongside cyber security skills, they demand more general IT and business skills, such as project management, risk assessment, network engineering, SQL, system administration, and technical support. This might be because the job requires light-touch knowledge and application of technical cyber security skills (e.g. for IT Technicians or Governance, Regulation and Compliance roles) or because the job role includes cyber security functions among other things (e.g. Network Engineers whose role is broader than just network security). Typical job titles, other than those already mentioned, include Computer Support, IT Support Analyst and Applications Analyst

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

Improving on the Burning Glass Technologies standard cyber security filter

Using the Burning Glass Technologies cyber security filter suggests that there were 188,264 cyber security job postings in the UK between September 2016 and the end of August 2019. However, we know that this filter is incomplete for the purposes of our analysis:

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

[22] This work was carried out using the Burning Glass Technologies Labour Insight tool: https://www.burning-glass.com/products/labor-insight/.
[23] See https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf.

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

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

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

1. Initial identification of more granular search terms to use on the Burning Glass Technologies platform (which we aligned to the Cyber Security Body of Knowledge, or CyBOK[24]).
2. Extracting an initial dataset from Burning Glass Technologies with over 300,000 job postings, using the identified inclusion/exclusion terms from step 1.
3. Reviewing the initial output and refining the inclusion/exclusion terms before extracting a second dataset from Burning Glass Technologies using the refined terms.
4. Supplementing the second dataset with Burning Glass Technologies’ own cyber security filter, which we used to distinguish between core cyber roles and cyber-enabled roles.
5. Confirming the final number of job postings within scope for this analysis (using the final, refined search strategy) with DCMS.

Our refined search criteria yielded 105,194 core cyber security roles, and a further 288,063 cyber-enabled roles. In total this comes to 393,257 job postings in scope for this strand (compared to Burning Glass Technologies’ own 188,264 job postings).

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

6.2 Metrics analysed

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

- The number of cyber security job postings in the UK, including a time-series analysis of the number of job postings posted each month over the last 3 years
- The industry sectors of the employers seeking people in cyber roles
- The geographic locations across the UK for these job postings
- Advertised job titles (to analyse the job roles most in demand)
- Job descriptions (to analyse the skills, experience, education, and qualifications being requested)
- The salaries or salary ranges being offered in these job postings

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

6.3 Strengths and limitations of the methodology

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

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

- **Volume and granularity** – we are able to analyse c.400,000 job postings from the last 3 years, exploring the specific jobs, skills and qualifications in demand. It can also drill down into areas such as the specific coding languages being sought. This method can uncover geographic clustering (down to specific towns and cities) of high demand and skills shortages for cyber professionals

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

- **Strong coverage** – the Burning Glass Technologies platform scrapes more than 40,000 online data sources[25]. Online postings reflect an estimated 85 per cent of jobs posted in the labour market (versus, e.g. print media)

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

- **Selection bias** – Burning Glass Technologies only scrapes free-to-use jobsites, which potentially leaves an (unknown) risk of bias if major employers are using closed platforms to post jobs, or other ways of recruiting such as networking and word-of-mouth. However, we believe this is offset by both the high volume and high coverage of the data that is available. This data still gives a strong insight into the trends and patterns in the labour market

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

[25] See https://www.burning-glass.com/about/faq/.

Appendix A: literature review

Introduction

This rapid evidence review examines recent literature on the cyber security skills shortage. The specific aim is to provide a review of the key studies and other publications that have emerged since the cut-off point for the original review in October 2018 (albeit with occasional reference to earlier studies that were not fully reviewed in the 2018 work).

The discussion is based upon an examination of a longlist of 47 sources in the main evidence review, plus a further 20 sources in relation to assessing actions being taken in the international context.

The review builds upon significant prior evidence that had already demonstrated a cyber skills shortage. As such, this update should not be expected to tell a fundamentally different tale, and it is too early for any resultant initiatives to have had an impact.

The state of the cyber security skills shortage

There continues to be no shortage of sources suggesting a Cyber Security Skills Shortage (CSSS) in the UK and more widely:

- **International: *EY's Global Information Security Survey 2018-19*** reports that 30% of organisations are struggling with skills shortages (placing the issue ahead of budgetary constraints, cited by 25%).[26] The situation is particularly acute in smaller organisations, where 56% indicate that they have skills shortages or budget constraints

- **International: *ISC2's 2018 Cybersecurity Workforce Study*** indicated 63% of organisations reporting a skills shortage, with a third of these categorising it as significant. The same study also quantified the shortage, indicating a global gap of 2.93 million (albeit with 2.14m of this residing in the Asia Pacific region)[27]

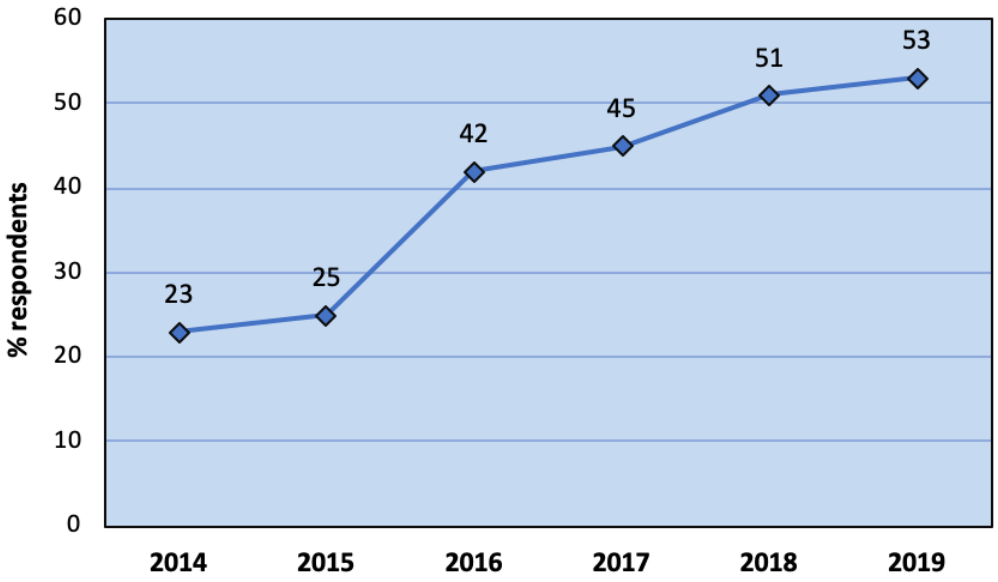
- **International: *Enterprise Security Group's annual survey*** of the challenges facing IT professionals has consistently cited a 'problematic shortage' of cyber security skills as its top issue. As Figure 1 illustrates, there is a year-on-year increase in the percentage of organisations citing it as an issue[28]

[26] EY. 2018. *Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19*. EYG no. 011483-18Gbl

[27] (ISC)^2. 2018. *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)^2 Cybersecurity Workforce Study 2018*. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx.

[28] Oltsik, J. 2019. "The Cybersecurity Skills Shortage Is Getting Worse", ESG Blogs, 10 January 2019. https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse

Figure 1: International organisations globally reporting a 'problematic shortage' of cyber security skills



- **UK: *The Security Profession in 2018/19*** report from the Chartered Institute of Information Security takes a slightly more granular view and differentiates between shortages in terms of skills (10%), resources (21%), experience (13%) and new entrants to the profession (5%)[29]. The resulting conclusion was that the main problem exists in terms of the number of people with skills rather than the ability of those that are available

- **UK: *The Open University's Bridging the Digital Divide*** report presents specific evidence across Great Britain, with a survey of 500 CTOs, HR Directors and HR Managers across England region, Wales and Scotland. This revealed that across all regions, a third of the business leaders reported that they did not have adequate cyber security capabilities within their organisation[30]

Somewhat surprisingly, further UK evidence from the ***Cyber Security Breaches Survey 2019***[31] suggests less of a problem, with 75% believing that the people dealing with cyber security in their organisation had the right cyber security skills and knowledge to do their job effectively and 79% believing that their organisation had enough people to manage the risks (meanwhile only 10% and 9% explicitly disagreed on these issues). These figures were broadly consistent, regardless of business size or whether the organisation was a business or charity. However, the response to a further statement ("I am not sure how our organisation should act on any advice I have seen or heard around cyber security"), was notably less confident, with 31% overall agreeing that they were not sure. Due to the wording of this statement, the result may reflect the respondents' own confidence about what to do, rather than imply that their cyber security team would not know how to act. Having said this, the findings are something of an outlier against the other evidence, and as the report itself observes: "Many organisations may assume they have the necessary skills, without fully understanding the technical requirements of the role".

[29] Wilson, P. 2019. *The Security Profession in 2018/19*. Chartered Institute of Information Security, July 2019.
[30] The Open University. 2019. *Bridging the Digital Divide*. June 2019. http://www.open.ac.uk/business/bridging-the-digital-divide
[31] DCMS. 2019. *Cyber Security Breaches Survey 2019. Statistical Release*. Department for Digital, Culture, Media & Sport, April 2019, London, UK.

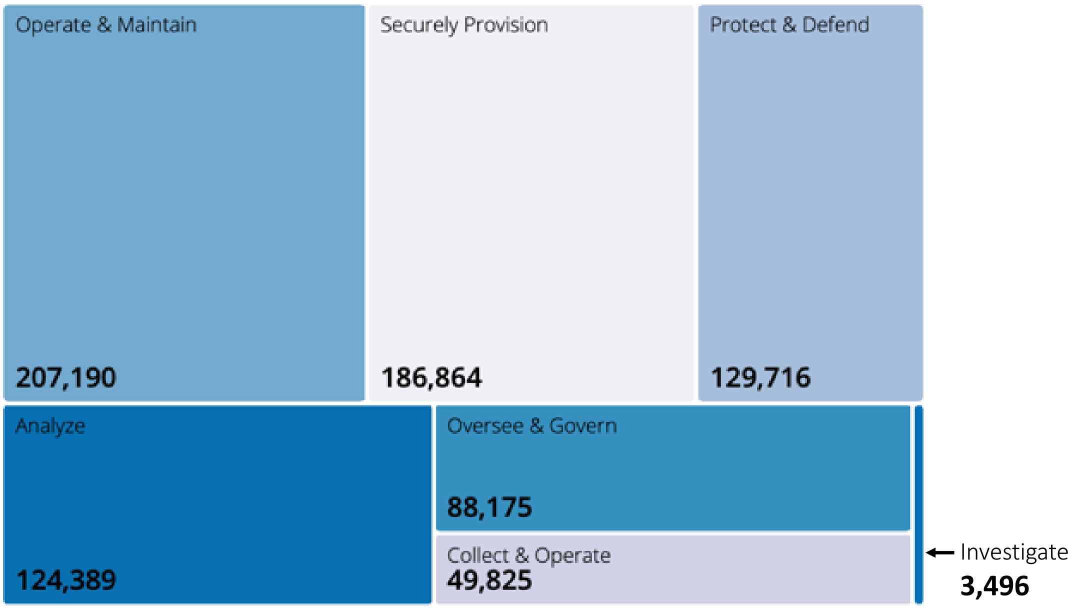
There is also clear ongoing evidence in terms of demand for cyber roles (as well as a lack of supply):

- **UK:** A June 2019 study from ***Burning Glass Technologies*** indicates that Cyber Security Knowledge tops the list of fastest growing skills in relation to Computer Support and Networking, with 5-year projected growth of 120% (notably, the linked area of Threat Intelligence and Analysis is next in the list, with 87%)[32]. The same report also highlights the shortfall between demand and supply for professional cyber security certifications. It cites the example of CISSP, where there are 4,455 annual openings but only 6,674 UK professionals holding this credential

- **UK:** As of April 2019, the ***UK Home Office's Shortage Occupation List*** specifically highlights "Cyber security specialist employed by a qualifying company, where the job requires a person with a minimum of 5 years' relevant experience and demonstrable experience of having led a team"[33]

- **USA:** A summary presented by ***Cyber Seek***, drawing upon US job vacancy and employability data from 2017/18, shows an average supply demand ratio of 2.3 (based upon almost 314K job openings against a current cyber workforce of just under 716K individuals)[34]. It is notable that the openings are unevenly distributed across a range of cyber security areas/roles, with Figure 2 summarising these according to the role classifications used in the NICE Workforce Framework[35]

Figure 2: Distribution of cyber security job openings



Source: Cyber Seek (2018)

Comparison can be made with recent UK job market findings widely reported from ***Indeed***[36], with the following table summarising the most advertised cyber security roles. It is notable that this broadly

[32] Nania, J., Bonella, H., Restuccia, D. and Taska, B. *No Longer Optional: Employer Demand for Digital Skills*. Burning Glass Technologies and Department for Digital, Culture, Media and Sport. June 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807830/No_Longer_Optional_Employer_Demand_for_Digital_Skills.pdf

[33] Home Office. 2019. "Immigration Rules Appendix K: shortage occupation list", 23 April 2019. https://www.gov.uk/guidance/immigration-rules/immigration-rules-appendix-k-shortage-occupation-list

[34] Cyber Seek. 2018. *Cybersecurity Supply/Demand Heat Map*. https://www.cyberseek.org/heatmap.html

[35] Newhouse, B., Keith, S., Scriber, B. and Witte. G. 2017. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST Special Publication 800-181. August 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[36] Ranger, S. 2019. "Cybersecurity jobs: These skills are most in demand and have the best pay", ZDNet, 22 May 2019. https://www.zdnet.com/article/cybersecurity-jobs-which-roles-are-most-in-demand-and-have-the-best-pay/

consistent with the Cyber Seek data, in terms of the specialists and engineers being likely to account for the operational and provisioning roles, and analysis and governance-related vacancies being present but less prominent.

The most in-demand cyber security roles in the UK market

Rank	Job title	Jobs per 1 million vacancies	Average salary
1	IT Security Specialist	538.5	£45,722
2	Security Engineer	192.6	£32,370
3	Security Consultant	117.6	£52,842
4	Information Security Analyst	115.4	£39,992
5	IT Auditor	66.3	£58,328

Source: Indeed (2019)

As a counterpoint to some CSSS percentages presented above, an extensive study supported by the ***Global Cyber Security Center*** presents its own review of the international evidence[37]. It confirms the widespread perception of a cyber security skills shortage, but questions the extent to which the nature of the shortage, and the drivers behind it, are properly understood (citing several methodological factors that can call some of the specific reports into question – including ambiguous questionnaires and poor generalisability of the current data). At the same time, it agrees that there is sufficient weight of overall evidence to confirm a mismatch between demand and supply of cyber security skills. The study points to the need for further research, particularly in terms of defining the nature of the shortage and means of measuring it. There is a need to understand the causes of the shortage, the experience levels at which shortage occurs, and whether it is qualitative and/or quantitative in nature.

Implications for primary research: It would be relevant to further investigate what *areas* of cyber security are perceived to be in short supply. Do employers feel they have more difficulty recruiting some skills more than others? There would potentially be an opportunity to rate the perceived severity of the shortage across different skills/role categories. Similarly, it would be pertinent to examine whether the shortages relate to specific levels of practitioners' experience.

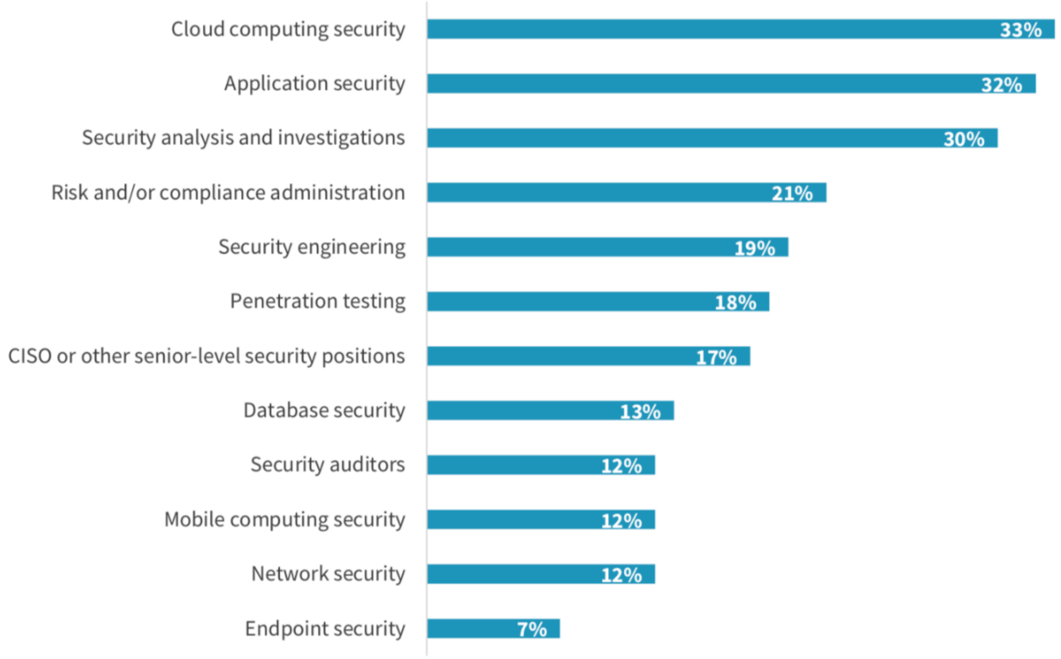
What skills are needed?

While the earlier Cyber Seek and Indeed sources reported vacancies, a worldwide survey of 267 cyber security professionals conducted by ***ESG/ISSA*** identifies the areas in which respondents reported their biggest cyber skills shortages[38]. As can be seen from the chart below, these are dominated by technical cyber security roles.

[37] De Zan, T. 2019. *Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions*. Global Cyber Security Center. February 2019. https://gcsec.org/mind-the-gap-the-cyber-security-skills-shortage-and-pubblic-policy-interventions-2/

[38] Oltsik, J. 2019. *The Life and Times of Cybersecurity Professionals 2018*. Research Report. Enterprise Security Group and Information Systems Security Associate, April 2019. https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

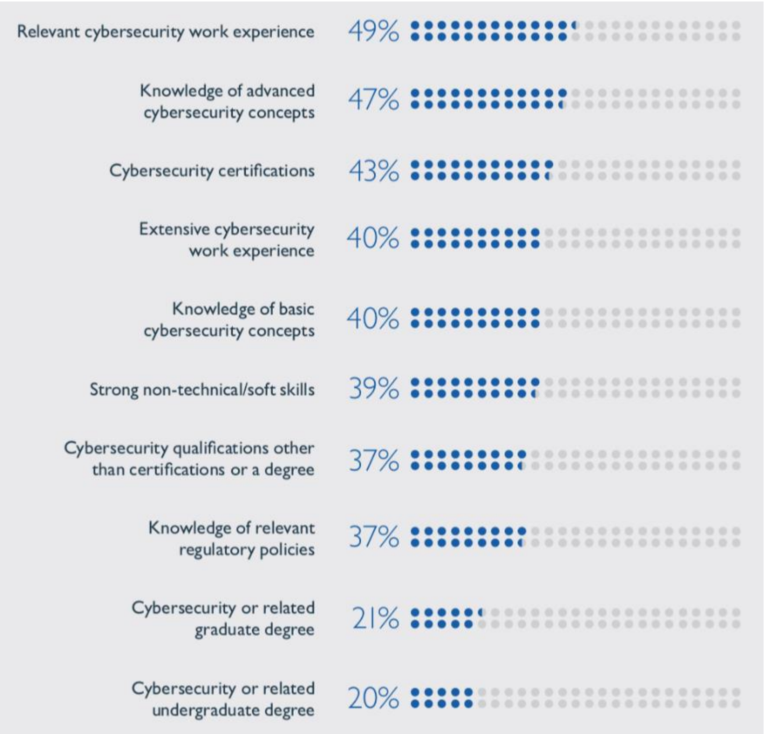
Figure 3: Areas of biggest cyber skills shortage



Source: Enterprise Security Group (2019)

The ***ISC2 Cybersecurity Workforce Study 2018*** presents an interesting assessment of the perceived importance of different forms of cyber security qualifications, with relevant work experience placed at the head of the list and academic degree qualifications at the bottom.

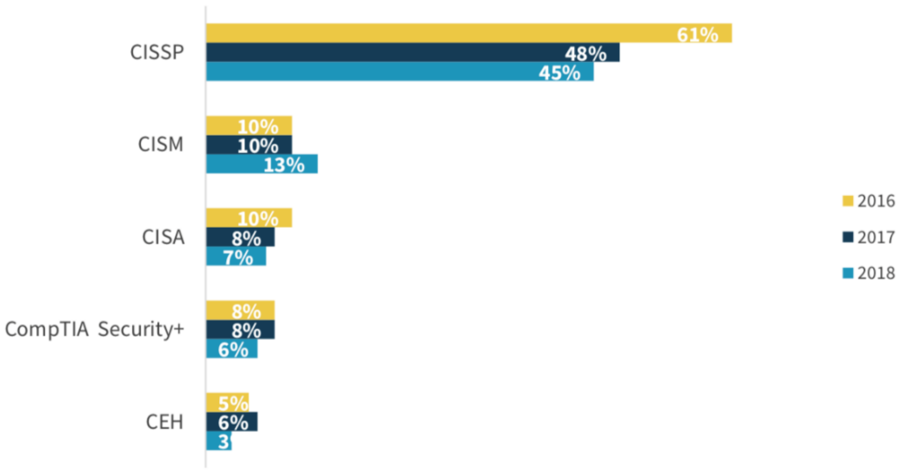
Figure 4: Importance of different cyber security qualifications



Source: ISC2 Cybersecurity Workforce Study (2018)

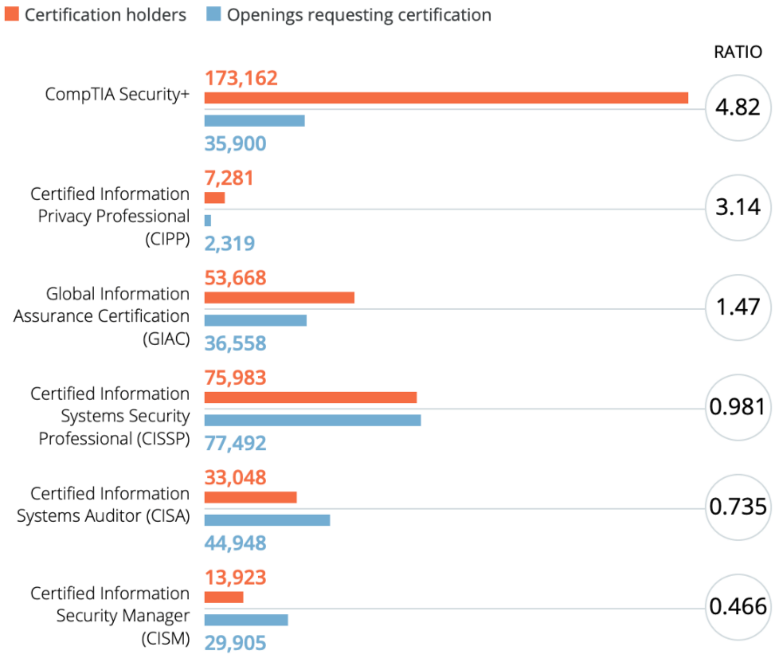
Aside from the general notions of knowledge and experience, the most prominent response relates to *Cyber security certifications*. However, with a myriad of certifications available, there is some variation of importance in this category. The ***ESG/ISSA study*** asked its respondents which of the cyber security certifications they held were most important in helping them to get jobs. This revealed ISC2's CISSP (Certified Information Systems Security Professional) certification as by far the most highly-rated (see Figure 5), and offers an interesting contrast to some further insight drawn from the ***Cyber Seek vacancy data*** (see Figure 6). This clearly suggests an over-supply of certifications such as CompTIA's Security+ and a notable under-provision in terms of the certifications in greater demand (which are also those denoting more experienced practitioners).

Figure 5: Cyber security certifications most important to employment



Source: Enterprise Security Group (2019)

Figure 6: Comparison of certification holders versus openings requiring the certification



Source: Cyber Seek (2018)

Having said all this, it is important to understand that cyber security professionals should not be characterised by technical skills alone. Two themes that emerge from the review are cyber security as a cross-disciplinary issue, and the need for business understanding and soft skills to support technical ability:

- **UK:** While it is most readily recognised in the context of IT and computer science, ***Collier and Martin*** note that the CSSS "extends to other disciplines and areas of expertise such as law, business strategy and public policy".[39] They note that a siloed approach to the issue can result in non-optimal solutions, and propose that cyber security teams should incorporate an "eclectic range of skillsets and experiences" in order to achieve an interdisciplinary viewpoint

- **International:** To quote ***ISACA's State of Cybersecurity 2019*** report[40]: "Currently, the most-prized hire in a cyber security team is a technically proficient individual who also understands business operations and how cyber security fits into the greater needs of the enterprise". This need to look beyond technical ability broadly aligns with earlier work from Dawson and Thomson, who propose 6 key traits that are likely to be required in the future cyber security workforce (namely systemic thinking, teamwork, continued learning, strong communication ability, a sense of civic duty, and a blend of technical and social skill)[41]. It is further echoed in a recent report from Symantec, *High Alert: Tackling Cyber Security Overload in 2019*[42]. This quotes Dr Steve Purser, Head of Core Operations at ENISA, who indicates that "the really good people in the security industry are far more than just technically skilled. Especially in the higher ranks, you will see people who have a good mix of technical and soft skills, which enables them to implement control frameworks that really work". This in no sense devalues the importance of the technical skills, but emphasises the importance of not seeking them in isolation

Implications for primary research: There is a clear challenge in knowing what the 'right skills' look like. Do employers feel that they understand what to look for in order to identify the skills they need (within their existing teams and among potential hires)? Do they feel that their existing security teams are able to relate to, and communicate with, the wider business? What do they look for during the recruitment process in terms of prior security experience, certifications, and wider skills? Are they prepared to recruit less experienced staff and enable them to undertake skills development?

Impacts resulting from lack of skills

Impact can be considered from the perspective of the business as well as effects upon the workers responsible for handling cyber security.

ISC2's 2018 Cybersecurity Workforce Study reported that 59% of respondents believed their organisation was facing "extreme or moderate risk" as a result of cyber security staff shortage.

In terms of impacts upon the workers themselves, Figure 7 presents a chart taken from the ***Symantec High Alert*** report. This is based upon a survey of 3,045 cyber professionals working in middle or upper leadership roles organisations (with the respondents split into approximately even groups from France, Germany and the UK). As can be seen, lack of skills is commonly reported, along with indications that

[39] Collier, J. and Martin, A. 2019. *Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand*. Working Paper Series – No. 10, Centre for Technology and Global Affairs, University of Oxford. March 2019. https://www.ctga.ox.ac.uk/article/beyond-awareness-breadth-and-depth-cyber-skills-demand

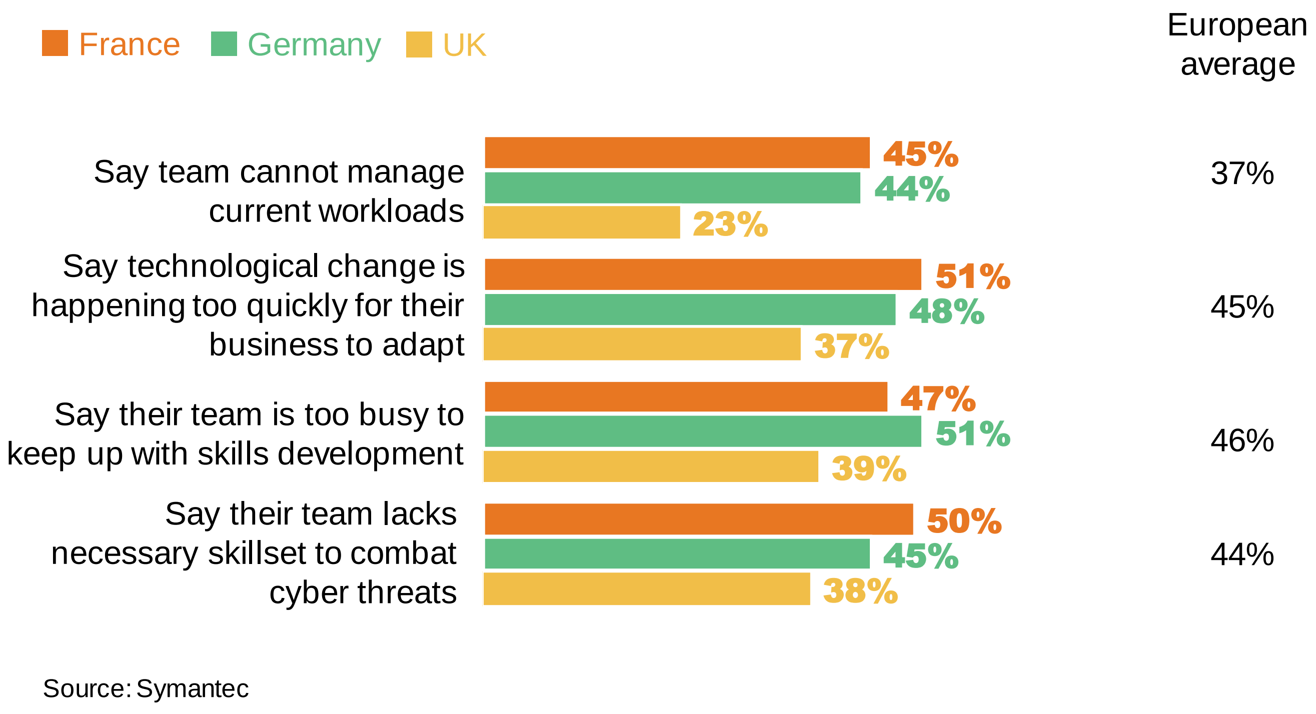
[40] ISACA. 2019. *State of Cybersecurity 2019 - Part 1: Current Trends in Workforce Development*. https://cybersecurity.isaca.org/state-of-cybersecurity

[41] Dawson, J. and Thomson, R. 2018. "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance", *Frontiers in Psychology*, 12 June 2018. https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full

[42] Symantec. 2019. *High Alert: Tackling Cyber Security Overload in 2019*. Symantec Corporation. https://resource.elq.symantec.com/LP=7421

the workload is too great to keep up with technology or maintain skills development. While the UK situation appears less severe than the average, all of the factors remain notable concerns.

Figure 7: Impacts of the skills shortage



Source: Symantec (2019)

Taking a wider geographic view, the aforementioned ***ESG and ISSA study*** found that three-quarters of organisations are experiencing a cyber skills shortage, with a third citing a significant impact. The most common areas of impact were:

- Increased workload on existing staff (66%)
- Inability to fully learn or utilise security technologies to their full potential (47%)
- The need to hire and train junior employees rather than hire experienced staff (41%)
- Limited time for cyber security staff to work with business units to align security with processes (40%)

There were also various other lower-rated factors of note, such as a lack of time for staff to address strategy and planning due to the demands of incident response, and a high rate of attrition and burnout amongst cyber security staff (with both of these factors cited by around a third of respondents).

The top 4 factors from the previous years are summarised in the following table from the report, revealing that some areas of impact have remained fairly consistent in this timeframe.

Top four areas of impact of cyber skills shortages

Top Four Factors Cited in 2016	Top Four Factors Cited in 2017	Top Four Factors Cited in 2018
Increased workload on existing staff	Increased workload on existing staff	Increased workload on existing staff
Need to hire and train junior staff, rather than experienced cyber security professionals	Need to hire and train junior staff rather than experienced cyber security professionals	Inability to utilise/learn some security technologies to their full potential
Inability to utilise/learn some security technologies to their full potential	Cyber security staff time is spent disproportionally on high priority events	Need to hire and train junior staff rather than experienced cyber security professionals
Higher attrition and turnover in cyber security staff	Cyber security team has limited time to work with business units	Cyber security team has limited time to work with business units

Source: ESG/ISSA (2019)

The ESG/ISSA report also notably points toward a "seller's market" for cyber security talent, with 76% of respondents indicating that they are solicited to change jobs by recruiters at least once a month, while almost half reported weekly contact. This, in turn, can have clear potential to impact the organisation, if it finds its existing cyber talent being lured away.

Implications for primary research: The skills shortage clearly has the potential to put pressure on existing teams. It would be relevant to further investigate whether organisations are feeling this and in what way(s) it is manifested. If the problem is experienced (or anticipated) are the organisations doing anything in response?

Gender and Diversity

All of the data at present indicates that both the current workforce and the pipelines of future talent are significantly skewed towards male participants:

- **International:** The ***ISC2 Cybersecurity Workforce Study 2018*** indicate that women represented 24% of the overall cyber security workforce

- **International:** The ***ISACA State of Cybersecurity 2019*** reported that 89% of respondents had more men than women in cyber security roles, with 51% reporting that there were significantly more men, and 15% indicating that their *entire* cyber security group was male. Almost a third (29%) of respondents indicated difficulties in retaining female cyber talent, and over half (56%) reported a lack of specific diversity programmes to support women cyber security professionals. Perceptions of career advancement opportunities for female cyber security professionals in the organisation were notably different depending upon who was asked – while 79% of men believed that women were offered the same opportunities, only 41% of women agreed

- **UK:** ***The Security Profession in 2018/19*** report from the Chartered Institute of Information Security suggests a similar picture, insofar as only 9% of the respondents were women

- **UK:** Higher Education Statistics Agency (HESA) data reported in a ***DCMS study of FE/HE provision*** reported that approximately 16% of students undertaking a cyber security degree in

2016-17 identified as female (with the proportion having remained steady over the past 3 academic years)[43]

In terms of contributing factors, international findings from Kaspersky Lab have suggested that 1 in 6 women believe that a career in cyber security would be 'dull', with the impression being formed and reinforced by terminology such as 'hacker' and the perception of those involved as geeks or nerds. The study observes that the use of more positive terminology (e.g. protector, guardian) would be more encouraging. The study also emphasises the lack of role models, and one of the key conclusions is that a cyber security careers need to be "promoted among young women, by women, and the industry as a whole"[44].

Where efforts are made, they indicate success. A recent UK example is the CyberFirst Girls Competition saw a total of 3,389 teams entering from 841 schools across the UK[45]. This suggests a clear willingness and potential for girls to engage if the opportunities are presented and promoted in a manner that connects with them.

Implications for primary research: A skewed workforce is likely to mean we are missing opportunities in terms of inputs, opinions, and perspectives. It would be relevant to investigate whether organisations recognise this as an issue and whether they consider themselves to have taken (or be likely to take) any steps to address it. Is it something that organisations feel they have a part to play in?

Addressing the skills shortage

Ensuring baseline cyber security skills

If organisations are lacking specialist cyber skills and the existing workforce is overloaded, then it is worth looking at what is *causing* the workload overhead and whether anything can be done to address it.

The aforementioned Symantec *High Alert* study reveals that the User Behaviour is the predominant driver of security workloads (cited by 37% of respondents), followed by Organisational politics/lack of attention to information security (22%). While there were 17 other categories, all were cited by less than 20% of respondents, and so the dominant issues driving security workload would appear to be aspects relating to (lack of) security culture.

This in turn points to a need to address baseline security awareness and compliance for end users, and so it is relevant to consider what is being done in this space.

- **UK/Ireland:** Interestingly, TechTarget's study of ***UK & Ireland 2019 IT Priorities*** revealed that end-user security training was identified as a priority by 32% of the 222 respondents[46]. This placed it at the top of the list of 20 security initiatives under consideration, ahead of cloud, IoT and mobile security, and a variety of other technical aspects

[43] Malan, J., Lale-Demoz, E. and Rampton, J. 2018. Identifying the Role of Further and Higher Education in Cyber Security Skills Development. Department for Digital, Culture, Media and Sport. December 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf

[44] Kaspersky Lab. 2018. *Beyond 11%: A study into why women are not entering cybersecurity*. November 2017. https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf

[45] NCSC. 2019. "Congratulations to the 2019 Girls Competition finalists", National Cyber Security Centre, 11 February 2019. https://www.cyberfirst.ncsc.gov.uk/congratulations-to-the-girls-competition-2019-finalists.

[46] TechTarget. 2019. *UK & Ireland 2019 IT Priorities*. TechTarget Infographic. https://media.bitpipe.com/io_10x/io_102267/item_1306461/2019_IT_Priorities_UKI_Infographic.pdf

- **UK:** The Department for Education has proposed ***National standards for essential digital skills***[47]. Based upon the earlier essential digital skills framework, these standards address the population as a whole, and define essential digital skills for work and life. They address 5 thematic areas, the fifth of which is 'Being safe and responsible online'. This includes specific skills statements relating to protecting privacy and protecting data. The skills are defined at Entry Level (for those with little or no experience of digital devices and the Internet) and Level 1 (for those with some experience but still lacking secure basic digital skills). For cyber security they encompass aspects such as awareness of online threats, secure configuration and use of devices and services, and safeguarding against loss or inappropriate sharing of data. The standards are relevant in the context of the (future) workforce, insofar as staff entering the workplace with baseline cyber literacy would raise the bar in terms of protection and thereby adjust the emphasis of what cyber security professionals in the organisation would be required to safeguard

- **Europe:** From a wider European perspective, ENISA's recent ***Cybersecurity Culture Guidelines***[48] highlights that organisations should be seeking to do more than raise awareness of cyber threats – they should be providing users with the skills to *deal* with them

Implications for primary research: Enhancing the cyber security awareness and behaviour of the general workforce has the potential to reduce the challenge facing the specialists. It would therefore be relevant to investigate the extent to which organisations feel that they currently have a cyber security-aware workforce, and whether they are making provision to support them in this respect. To what extent do they perceive that their wider workforce is (directly or indirectly) causing workload impacts for their cyber specialists?

Recognising and retaining cyber security talent

A recurring theme in several recent studies is that organisations could be looking at their cyber security skill requirements in different ways and doing more to support retention of talent.

- **UK:** Drawing upon opinions from 60 industry experts, InfoSecurity Magazine's ***State of Cybersecurity Report 2019*** flags two aspects that many organisations could alter in order to recruit and develop talent[49]:

  − More realistic hiring processes, reducing the expectation new hires should be immediately deployable at a high level and are pre-equipped with the full technical background
  − More resourcing for training to upskill junior people into senior security roles, which would position them to make better decisions without firstly having to accumulate years of prior experience

  A further commentator went as far as to assert that there is no talent deficit and that the situation could be addressed if it was approached differently ("there are tons of people who would like a job in cyber and we shouldn't make it more difficult for them to get one")

[47] Department for Education. 2019. *National standards for essential digital skills*. April 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/796596/National_standards_for_essential_digital_skills.pdf

[48] ENISA. 2019. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. European Network and Information Security Agency. December 2018. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

[49] Raywood, D. 2019. *State of Cybersecurity Report 2019*. June 2019. https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2019-1/

- Reflecting a view from IBM, Batten suggests ways of empowering existing in-house cyber security talent, based upon[50]:
  - Creating a mentoring programme, to enable new hires to be supported by established cyber security staff
  - Joining a professional organisation (e.g. ISACA, SANS or ISSA), in order to keep up to date with trends and developments
  - Sharing best practices via community engagement, to enable interaction with a wider group of subject matter experts

- Matthews flags the need for creativity on the part of HR teams looking to manage the skills situation for their organisations[51]. This again includes the idea of developing and growing skills internally rather than external recruitment for non-urgent positions, as well as recognising that workplace initiatives can be used to support talent retention. Given that the skills shortage is a recognised cause of increased workload and resultant stress for current workers, initiatives such as free gym membership or other interventions supporting staff welfare could be considered

- **Europe:** Also linking to the welfare of the cyber workforce, the ***ENISA Cybersecurity Culture Guidelines*** highlights that organisations should be looking after their staff in order to guard against burnout, and ensuring that there are opportunities for training and personal growth. Staff in incident response teams and security operations centres are highlighted for particular consideration, given the importance (and potentially stressful nature) of their role in protecting the organisation

The points around developing talent and increased training raise the question about how organisations can make space for this given the demands already placed upon the workforce. ***Symantec's High Alert report*** acknowledges this, and highlights the need for "complementary alternatives that can help free up time for skills development and ease the recruitment burden". The following alternatives are suggested:

- Rationalisation (using integrated cyber system so that there are fewer distinct platforms/solutions to be managed)
- Embedded Security (so that it is provided within services such as web and email, without user intervention)
- Automation (to remove manual/repetitive aspects, as well as to leverage AI and Machine Learning to aid protection)
- Externalisation (using managed service providers to handle key aspects)

While none represent a panacea, they have potential to assist in the context of a fully-considered security strategy.

Implications for primary research: This links back to the earlier suggestion that the survey should investigate whether organisations feel they are making provisions to support a potentially overloaded workforce. Opinions and activities could be explored in relation to hiring strategy, mentoring, and welfare initiatives.

[50] Batten, W. 2019. "Think Inside the Box to Bridge the Cybersecurity Skills Gap", IBM SecurityIntelligence, 25 March 2019. https://securityintelligence.com/think-inside-the-box-to-bridge-the-cybersecurity-skills-gap/
[51] Matthews, K. 2018. "Recruiting in the age of the cyber security skills gap: challenges to overcome", Information Age, 3 December 2018. https://www.information-age.com/recruiting-in-the-age-of-the-cyber-security-skills-gap-123476988/

Supporting the skills pipeline

Reflecting on the establishment of the UK's National Cyber Security Centre, Hannigan highlights the ongoing challenge of increasing the talent pipeline to support cyber, and the need for "strategic interventions in the education system to effect long-term change"[52]. He suggests that a specific focus should be upon fostering STEM (science, technology, engineering and maths) skills at school level, supported by emphasis in the national curriculum and training for teachers. Hannigan observes that while initiatives such as *CyberFirst* and the *Cyber Security Challenge UK* have been positive, they are far from achieving the scale that has been achieved in the Israeli cyber education programme, which the UK activities have used as a point of reference.

Picking up on Hannigan's comment about STEM, and looking at the nature of the pipeline at present, it is possible to observe recent increases in the proportion of students taking STEM-based subjects, both at school and in higher education:

- At GCSE level across the UK, there were 2018 increases in entries into the individual sciences (23% in biology, 18.6% in chemistry and 17.2% in physics) and into computing (11.8%), although mathematics saw a 3% drop[53]
- At A Level, the most significant rise in 2018 was in computing (with a 23.9% increase in candidates), while biology, chemistry, mathematics and physics all saw more modest increases, in the 2.5% to 3.5% range[54]
- In Higher Education, there were 2017/18 increases in students studying biological science (3%), physical sciences (1%), mathematical sciences (2%) and computer science (6%)[55], with all but physical sciences also having increased the prior year

Additionally, DCMS's prior investigation of cyber skills development reports on the provision of cyber security courses in the higher education (HE) and further education (FE) sectors. Figure 8 contrasts the number of students studying on Information Communications Technology (ICT) and cyber security courses at the FE and HE levels in the 2016/17 academic year, and has a clear relationship to feeding the pipeline that could address skills shortages. While the inclusion of cyber security content into programmes will not directly develop cyber security professionals and practitioners, it will help to ensure that more graduates are aware of the issue and better positioned to develop further.

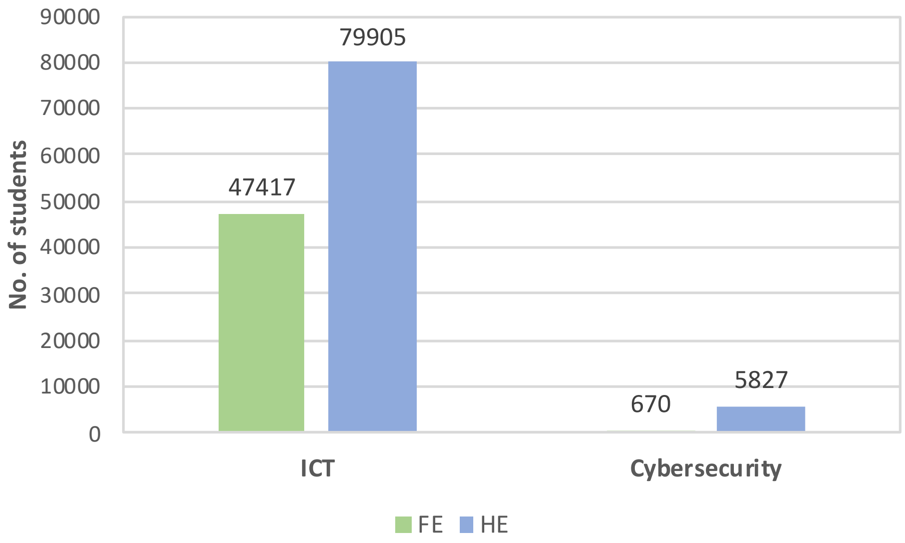
[52] Hannigan, R. 2019. *Organising a government for Cyber - The Creation of the UK's National Cyber Security Centre*. Occasional Paper, Royal United Services Institute for Defence and Security Studies, February 2019. https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf

[53] JCQ. 2018. *GCSE (Full Course) Outcomes for all grade sets and age breakdowns for UK candidates - Results Summer 2018*. Joint Council for Qualifications. 23 August 2018. https://www.jcq.org.uk/examination-results/gcses/2018/main-results-tables

[54] CaSE. 2018. "Rise in STEM popularity amongst A-level students", Campaign for Science and Engineering, 18 August 2018. http://www.sciencecampaign.org.uk/news-media/case-comment/rise-in-stem-popularity-amongst-a-level-students.html

[55] HESA. 2019. *Higher Education Student Statistics: UK, 2017/18 - Subjects studied*. Higher Education Statistics Agency, 17 January 2019. https://www.hesa.ac.uk/news/17-01-2019/sb252-higher-education-student-statistics/subjects.

Figure 8: Students studying ICT and cyber security courses in Further and Higher Education (2016/17)



Having said this, it should be acknowledged that not all cyber professionals need or have an ICT background. Many current practitioners are working effectively having come into the profession via non-IT and non-cyber routes, and this should continue to be the case (which also relates back to the earlier observation about the cross-disciplinary nature of cyber security). This recognition already exists within initiatives such as the NCSC's *CyberFirst Bursary* and *CyberFirst Degree Apprenticeship* schemes, both of which accept applications from candidates with non-IT (and indeed non-STEM) backgrounds[56].

In the UK, a ***2019 report by EDUCAUSE*** looks at the IT workforce more generally and makes interesting observations around what those recruiting and working with IT staff may be looking for in terms of non-technical, soft skills, such as communication, teamwork and attitude[57]. This has implications for the cyber security workforce, again highlighting the need for cyber professionals to be suitably versed in Skills Group J (i.e. Management, Leadership, Business and Communications) from the IISP Skills Framework. The same report additionally observes that technical skills will change in ways that cannot currently be foreseen and that those required in a decade will have little resemblance to what organisations need today. This highlights a need for agility in academic programmes and training provision, as well as the need to support Continuing Professional Development (CPD) courses within the cyber workforce.

Implications for primary research: Cyber security is not exclusively about technical skills and consequently those contributing to it should not be exclusively from IT or STEM backgrounds. It would be relevant to explore the extent to which organisations understand and share this view.

Industry and Professional Initiatives

IISP Frameworks

While the CSSS is often referred to in generic terms, it is clear that cyber security is a diverse topic, requiring a range of supporting skills. As such, it is useful to have a frame of reference to understand what the underlying skills actually *are*, which can then be used to determine how they relate to the areas

[56] See https://www.ncsc.gov.uk/section/education-skills/11-19-year-olds#section_4
[57] EDUCAUSE. 2019. *Technology in higher education: shaping the future IT workforce*. EDUCAUSE and Jisc Joint Report. 9 April 2019. https://www.jisc.ac.uk/reports/technology-in-higher-education-shaping-the-future-it-workforce#

of short supply. Useful contributions here are offered by the **Chartered Institute for Information Security** - formerly the Institute of Information Security Professionals (IISP) - which has devised a series of frameworks that can assist in understanding and expressing the needs. These individually seek to address Skills, Knowledge and Roles.

Providing overall context is the *IISP Skills Framework*, version 2.3 of which was released in November 2018[58]. This defines 32 Skills Groups (split across 10 thematic sections) which collectively encompass a range of technical and non-technical skills in cyber security, as well as more general business and professional skills (the demand for which has been highlighted other evidence). Each of the skills can then be rated at 6 levels, ranging from basic knowledge through to denoting a lead practitioner. The key opportunity arising from this is the ability to map against the framework:

- Individuals can map themselves in terms of current and target levels
- Roles and vacancies can be mapped in terms of the skills they need
- Organisations can map their teams in order to understand existing skills and gaps
- Qualifications and certifications can be mapped in terms of their coverage

While the Skills Framework expresses what someone should be able to do, the IISP Knowledge Framework[59] focuses upon what they need to know in order to do so. It specifically aims to define the knowledge required by Cyber Security professionals at levels 1 and 2 (i.e. to cover knowledge and understanding of basic principles). It is less relevant in the context of this review but is mentioned for completeness.

The most recent contribution is the accompanying *IISP Roles Framework*[60]. This takes eleven common roles (including CISO, Pen Tester, Security Architect, and Threat Analyst) and maps them to the primary and secondary skills areas that are considered relevant (as well as the qualifications and experience that one might expect to see). The Roles Framework is in a pre-release version at the time of writing but seems likely to provide a useful reference resource as it matures.

Implications for primary research: The fact that there is a (newly chartered) UK professional body, the UK Cyber Security Council, specifically linked to cyber security raises the question of whether organisations are looking for (or would consider) such a professional membership as a relevant indicator in their hiring process. It would also be relevant to examine awareness of the related Frameworks, and whether these are considered to be something that the organisations would aim to use.

The Cyber Security Body Of Knowledge (CyBOK)

The CyBOK is an NCSC-funded initiative aiming to develop "A comprehensive Body of Knowledge to inform and underpin educational and professional training for the cyber security sector" (see www.cybok.org). More specifically, it is intended as *guide* to the body of knowledge that already exists, mapping this to a series of specific cyber security Knowledge Areas defined by the project.

[58] IISP. 2018. *IISP Skills Framework - Version 2.3*, November 2018. The Institute of Information Security Professionals. https://www.iisp.org/iisp/Development/Our_Frameworks/IISP_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx.

[59] IISP. 2019. *IISP Knowledge Framework - Version 1.1.1*, March 2019. The Institute of Information Security Professionals. https://www.iisp.org/imis15/iisp/About_Us/Our_Knowledge_Framework/Download_IISP_Knowledge_Framework/iisp/About_Us/Download_IISP_Knowledge_Framework.aspx

[60] IISP. 2019. *IISP Roles Framework - Version 0.3*, March 2019. https://www.iisp.org/iisp/Development/Our_Frameworks/IISP_Roles_Framework/iisp/About_Us/Our_Roles_Framework.aspx.

The CyBOK work commenced in 2017, and an overview of the 19 top-level Knowledge Areas was included in the original review. The full set of 19 Knowledge Areas have now been released as v1.0. This gives confidence that the project will ultimately deliver full releases across the full set of areas.

The CyBOK is relevant as it will become the frame of reference for other activities, such as the NCSC's certification scheme for Bachelors and Masters degrees in cyber security.

Implications for primary research: Again, it would be relevant to explore awareness of the initiative and the contribution that it could make to the hiring process.

International initiatives

Having reviewed the evidence in general terms, and established an ongoing and internationally recognised concern, this section aims to examine other nations approaches to addressing their current cyber security skills gap and what can be learnt from them.

From the general evidence review, it was identified that the '*Mind the Gap*' report from the ***Global Cyber Security Center*** had already examined the cyber security policies of 12 countries (Australia, Estonia, France, Japan, Netherlands, Norway, Singapore, South Korea, Sweden, Switzerland, United Kingdom, United States). These dated from 2015-2018 and consistently highlighted a need for cyber skills, plus (in most cases) a concern regarding shortfall in the available supply. The report also summarised what the countries are doing in order to respond to the shortages, with the focus across 4 areas:

- Primary and secondary education
- Vocational education and apprenticeships
- Higher education and research
- Workforce

Those countries with longer-standing cyber security strategies (e.g. Japan and the US, alongside the UK) are shown to have more established and wide-ranging programmes in place to support them. In the education space, the efforts are found to be more prominently focused around higher education and research, with various countries establishing programmes such as academic centres of excellence, certified degrees, and direct funding of research. In the workforce context, efforts are directed towards both recruitment and retraining.

Given that the aforementioned review was itself relatively recent, a further assessment would seem unlikely to reveal significantly different findings. Nonetheless, the topic space is dynamic and there have indeed been some recent developments from some of the countries listed above, plus others that were sampled. As such, the sections below present related summaries relating to activities from 10 individual country approaches, as well as a summary level look at the situation regarding compliance with cyber awareness and education recommendations in the European context from ENISA. The selected countries encompass the Five Eyes (Australia, Canada, New Zealand, United Kingdom, United States) plus a sample of other countries that were highlighted during the evidence review and/or considered of potential interest (Ireland, Israel, Norway, South Africa, South Korea).

Australia

The Australian government has a range of cyber-related initiatives, within the over-arching context of the ***2016 Cyber Security Strategy***, to which the government committed $230M. The most notable aspects from a skills and workforce perspective are as follows[61]:

- Academic Centres of Cyber Security Excellence (ACCSE) programme – encourages more students to study cyber security and related courses, supported by $1.9M of Cyber Security Strategy funding, shared between the University of Melbourne and Edith Cowan University
- The Cyber Security National Program – AustCyber (The Australian Cyber Growth Network) has assisted the development of cyber security qualifications at TAFE (Technical and Future Education) providers
- Women in Cyber – an initiative seeking to address the underrepresentation of women in Australia's cyber security workforce

Linked to this, the 2018 update of ***Australia's Cyber Security Sector Competitiveness Plan***[62] indicates progress in relation to activities to increase the awareness of cyber security careers:

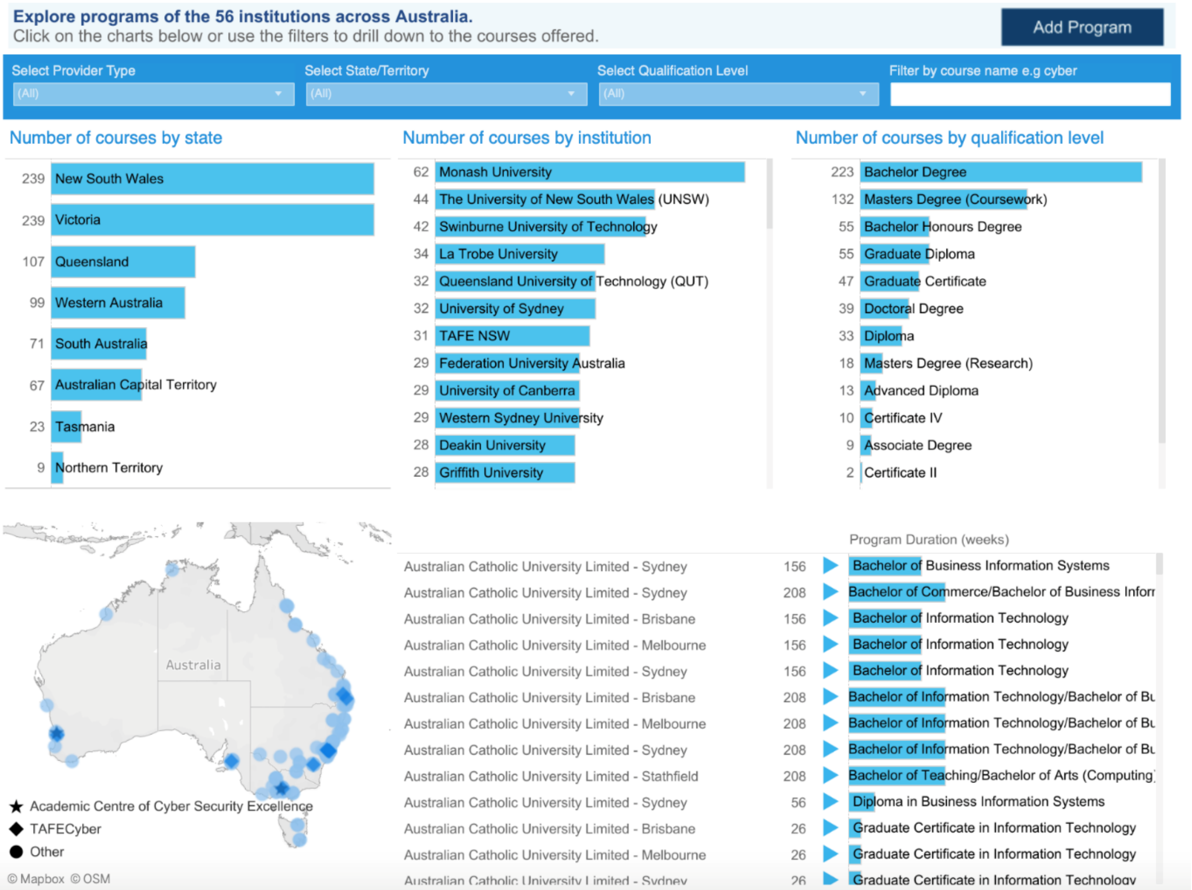
- "AustCyber has begun releasing a suite of interactive dashboards on cyber security careers, training opportunities, roles and career paths
- "LifeJourney, a new online career mentoring offering in Australia, has launched a Cyber Schools Challenge in various States. The programme seeks to ignite high school students' interest in cyber security careers"

The dashboards can be found at https://www.austcyber.com/resources/education-dashboards, and offer an interesting opportunity to explore security roles (based upon the structure proposed by the NICE Framework), available education opportunities, and the availability of cyber security challenge competitions. Figure 9 illustrates the Education Map, which allows interactive exploration of cyber security education offerings at different providers across the country, allowing filtering by various characteristics, including region and level of study.

[61] Australian government. *government Initiatives – Cyber Security*. Department of Industry, Innovation and Science. https://www.industry.gov.au/data-and-publications/australias-tech-future/government-initiatives#cyber-security

[62] AustCyber. 2018. *Australia's Cyber Security Sector Competitiveness Plan - 2018 Update*. 27 November 2018. https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2018

Figure 9: AustCyber's Education Map dashboard



Explore programs of the 56 institutions across Australia.
Click on the charts below or use the filters to drill down to the courses offered.

Number of courses by state

239	New South Wales
239	Victoria
107	Queensland
99	Western Australia
71	South Australia
67	Australian Capital Territory
23	Tasmania
9	Northern Territory

Number of courses by institution

62	Monash University
44	The University of New South Wales (UNSW)
42	Swinburne University of Technology
34	La Trobe University
32	Queensland University of Technology (QUT)
32	University of Sydney
31	TAFE NSW
29	Federation University Australia
29	University of Canberra
29	Western Sydney University
28	Deakin University
28	Griffith University

Number of courses by qualification level

223	Bachelor Degree
132	Masters Degree (Coursework)
55	Bachelor Honours Degree
55	Graduate Diploma
47	Graduate Certificate
39	Doctoral Degree
33	Diploma
18	Masters Degree (Research)
13	Advanced Diploma
10	Certificate IV
9	Associate Degree
2	Certificate II

	Program Duration (weeks)	
Australian Catholic University Limited - Sydney	156	Bachelor of Business Information Systems
Australian Catholic University Limited - Sydney	208	Bachelor of Commerce/Bachelor of Business Inforr
Australian Catholic University Limited - Brisbane	156	Bachelor of Information Technology
Australian Catholic University Limited - Melbourne	156	Bachelor of Information Technology
Australian Catholic University Limited - Sydney	156	Bachelor of Information Technology
Australian Catholic University Limited - Brisbane	208	Bachelor of Information Technology/Bachelor of Bu
Australian Catholic University Limited - Melbourne	208	Bachelor of Information Technology/Bachelor of Bu
Australian Catholic University Limited - Sydney	208	Bachelor of Information Technology/Bachelor of Bu
Australian Catholic University Limited - Stathfield	208	Bachelor of Teaching/Bachelor of Arts (Computing)
Australian Catholic University Limited - Sydney	56	Diploma in Business Information Systems
Australian Catholic University Limited - Brisbane	26	Graduate Certificate in Information Technology
Australian Catholic University Limited - Melbourne	26	Graduate Certificate in Information Technology
Australian Catholic University Limited - Sydney	26	Graduate Certificate in Information Technology

The 2018 update also indicates progress indicated in terms of building up educational provision in Technical and Further Education institutions (TAFEs) and universities, with several institutions highlighted as having developed or launched related programmes.

Canada

The **National Cyber Security Strategy**[63] highlights the need for skills, recognising that better provisions are needed across the population ("from our children to our elderly"), and across organisations ("from our small and medium business owners to our law enforcement agencies and corporate executives"). It is also recognising that attracting and retaining the required talent is difficult as a result of short supply.

In terms of addressing the issue, reference is made to the necessity of "working together across governments, academia, and the private sector" to address the cyber skills gap. More specifically, it makes broad reference to the need to encourage more students to move into STEM fields, as well as encouraging graduates from STEM and other disciplines (e.g. management, psychology or sociology) "to specialise in the skills needed for cyber security jobs". The Strategy also refers to the importance of attracting such multidisciplinary talent from abroad as well as domestically. Beyond this, however, the document does not articulate any specific steps toward achieving the goals.

[63] Public Safety Canada. 2018. *National Cyber Security Strategy - Canada's Vision for Security and Prosperity in the Digital Age.* 12 June 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Ireland

A draft public consultation document on the **National Cyber Security Strategy** was published in March 2019[64]. This recognises the critical importance of a skilled cyber security workforce, combined with the dual challenges of an existing skills shortage and fewer young people regarding cyber security as a career path.

A 3-year Cyber Security Skills Initiative was launched in October 2018, with the aim of developing awareness, bridging the skills gap and setting standards for skills and competencies for Cyber Security roles. Focus areas will include CPD and attracting women into the sector, and Skillnet Ireland anticipates delivering related training to >5,000 people in the industry during the 3-year period.

The consultation poses questions over what can be done to improve the availability of skilled workers, as well as supporting the relationship between academia and industry in order to foster and maintain a skills pipeline.

Norway

The context is set by the **National Cyber Security Strategy for Norway**. The List of measures to support the strategy includes a specific recommendation to “Include cyber security in the corporate culture”[65]. This recognises that employees at all levels have a role to play and emphasises the need for companies to ensure that their staff have the necessary knowledge and skills to do so. Suitable training tracks should be available for all employees at all levels, and those supporting key services require specific attention.

Additional reference is made to a **National Strategy for Cyber Security Competence** (only available in Norwegian). According to a summary at Eurydice, “The strategy sets out conditions for long-term competence building, encompassing national capacity in the fields of research, development, education, and measures designed to raise awareness in the business community and among the general public”[66]. It is noted that capacity in ICT-related education programmes, including digital security, has been increased by 1500 in order to meet demand.

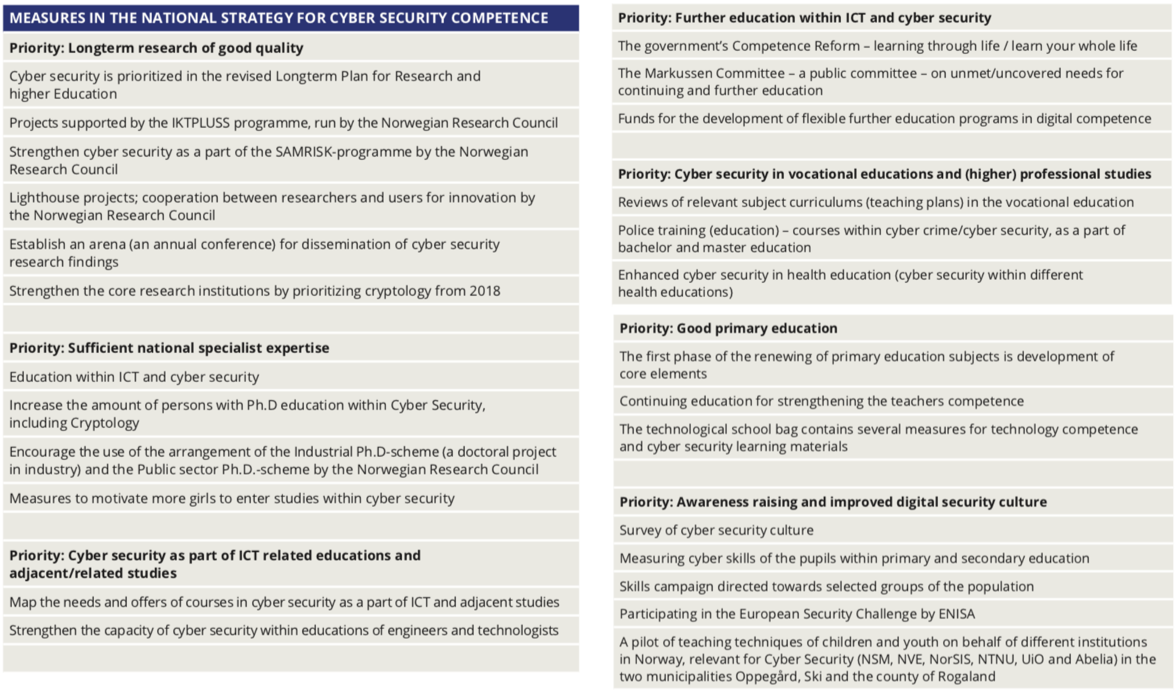
A series of resultant measures from the competence strategy are summarised below.

[64] Department of Communications, Climate Action and Environment. 2019. *National Cyber Security Strategy Draft Public Consultation*, March 2019. https://www.dccae.gov.ie/en-ie/communications/consultations/Documents/87/consultations/National%20Cyber%20Security%20Strategy%20Consultation%20Document.pdf

[65] Norwegian Ministries. 2019. *List of measures – National Cyber Security Strategy for Norway*. 30 January 2019. https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/

[66] Eurydice. 2019. “Norway - National Reforms related to Transversal Skills and Employability”, 29 March 2019. https://eacea.ec.europa.eu/national-policies/eurydice/content/national-reforms-related-transversal-skills-and-employability-48_en

Figure 10: Priorities from the Norwegian National Strategy for Cyber Security Competence



MEASURES IN THE NATIONAL STRATEGY FOR CYBER SECURITY COMPETENCE
Priority: Longterm research of good quality
Cyber security is prioritized in the revised Longterm Plan for Research and higher Education
Projects supported by the IKTPLUSS programme, run by the Norwegian Research Council
Strengthen cyber security as a part of the SAMRISK-programme by the Norwegian Research Council
Lighthouse projects; cooperation between researchers and users for innovation by the Norwegian Research Council
Establish an arena (an annual conference) for dissemination of cyber security research findings
Strengthen the core research institutions by prioritizing cryptology from 2018
Priority: Sufficient national specialist expertise
Education within ICT and cyber security
Increase the amount of persons with Ph.D education within Cyber Security, including Cryptology
Encourage the use of the arrangement of the Industrial Ph.D-scheme (a doctoral project in industry) and the Public sector Ph.D.-scheme by the Norwegian Research Council
Measures to motivate more girls to enter studies within cyber security
Priority: Cyber security as part of ICT related educations and adjacent/related studies
Map the needs and offers of courses in cyber security as a part of ICT and adjacent studies
Strengthen the capacity of cyber security within educations of engineers and technologists

Priority: Further education within ICT and cyber security
The government's Competence Reform – learning through life / learn your whole life
The Markussen Committee – a public committee – on unmet/uncovered needs for continuing and further education
Funds for the development of flexible further education programs in digital competence
Priority: Cyber security in vocational educations and (higher) professional studies
Reviews of relevant subject curriculums (teaching plans) in the vocational education
Police training (education) – courses within cyber crime/cyber security, as a part of bachelor and master education
Enhanced cyber security in health education (cyber security within different health educations)
Priority: Good primary education
The first phase of the renewing of primary education subjects is development of core elements
Continuing education for strengthening the teachers competence
The technological school bag contains several measures for technology competence and cyber security learning materials
Priority: Awareness raising and improved digital security culture
Survey of cyber security culture
Measuring cyber skills of the pupils within primary and secondary education
Skills campaign directed towards selected groups of the population
Participating in the European Security Challenge by ENISA
A pilot of teaching techniques of children and youth on behalf of different institutions in Norway, relevant for Cyber Security (NSM, NVE, NorSIS, NTNU, UiO and Abelia) in the two municipalities Oppegård, Ski and the county of Rogaland

Israel

Israel is widely regarded as one of the most successful cyber security economies, and is in many ways the reference point for other national approaches.

A recent article identifies 3 ways in which Israel has provided a particular environment for fostering cyber security talent and activity[67]:

- **Mandatory Military Service** – All citizens must serve approximately 2 years in the Israel Defense Forces (IDF), a long-standing model (since 1949) that has evolved from cryptography and signals intelligence to focus on "military-grade" cyber skills. It is claimed that 90% of adult Israelis working in the high-tech sector have undertaken military service
- **Unit 8200 –** The country's signals intelligence function similar to GCHQ or NSA, which has the opportunity to screen IDF entrants before they enter the service and take its pick of the candidates. The top talent can therefore be steered towards cyber security activities
- **Government Planning and Investment –** The level of investment sends a clear message of cyber security as a national priority (e.g. the Israeli Innovation Authority, the Ministry of Economy and Industry, and the National Cyber Directorate recently announced a further $24m programme of funding, adding to existing innovation centres and incubators that have been established)

Such activities are supplemented by further initiatives to identify and engage talent, such as after-school clubs run by defence agencies. Additionally, former leaders of Unit 8200 have created Team8 (see www.team8.vc), which describes itself as a "think-tank and company creation platform" and acts as an

[67] Petrella, S. 2019. "How Israel Closed The Cybersecurity Skills Gap", CyberVista, 29 November 2018. https://www.cybervista.net/how-israel-closed-the-cybersecurity-skills-gap/

incubator for cyber security companies. Such activities illustrate how cyber security is receiving particular emphasis in wider society, but supported and influenced from IDF sources.

It is clear that several elements here would not be easily replicable in other countries (e.g. as the approach depends heavily upon conscription and has evolved from a long-standing position), but there are elements that can be adapted to suit other contexts (e.g. GCHQ funding students on the basis of them going to work in cyber security areas).

New Zealand

The new ***Cyber Security Strategy 2019***, published in early July, identifies 5 priority areas, the first 2 of which pertain to cyber awareness and skills amongst the workforce[68]:

- Cyber security aware and active citizens
- Strong and capable cyber security workforce and ecosystem

The former refers to general cyber security awareness amongst the population, and the need to support them via associated awareness and education. Meanwhile, the cyber security workforce priority highlights a series of points in which related action should be taken:

- Incentivising and increasing the supply of skilled cyber security workers
- Supporting the expansion of roles and opportunities for cyber security workers
- Incentivising the growth of the cyber security industry in New Zealand
- Supporting industry and professional organisations to promote responsible management of cyber security across their organisations and workplaces
- Encouraging the development of a world-class cyber security academic research community
- Supporting high-quality cyber security research and encouraging links between academia and industry

The document does not go into further detail about how these will be achieved, but it is clear that the general principles expressed tend to echo the themes already being enacted through initiatives in other countries.

Singapore

Singapore’s Cyber Security Strategy is based around 4 pillars, the third of which is ‘Developing a vibrant cyber security ecosystem’. Within this, a number of initiatives were pursued in 2018 in relation to the enhancement of the cyber security capability base and talent pool. Quoting from the ***Singapore Cyber Landscape 2018*** report, the following initiatives are of potential note, all of which were established or launched in 2018[69]:

- **Lean LaunchPad Programme Cybersecurity Track:** a 10-week experiential learning programme to equip cyber security researchers and young start-ups with the necessary networks, tools, and market validation to bring their inventions to market.
- **National Satellites of Excellence (NSoEs).** Anchored in local universities, these aim to build and consolidate local research strengths in domains of national interest (specifically Trustworthy

[68] New Zealand government. 2019. *New Zealand’s cyber security strategy 2019 - Enabling New Zealand to thrive online*. Department of the Prime Minister and Cabinet (DPMC), July 2019. https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf
[69] CSA. 2019. *Singapore Cyber Landscape 2018*. Cyber Security Agency of Singapore, June 2019. https://www.csa.gov.sg/~/media/csa/documents/publications/csasingaporecyberlandscape2018.pdf

Software Systems; Mobile Systems Security & Cloud Security; and Design Science and Technologies for Secure Critical Infrastructure).

- An annual **Youth Cyber Exploration Programme (YCEP)** with Singapore Polytechnic, to inculcate student interest in cyber security
- A Cyber Security **Career Mentoring Programme (CCMP)** with the Singapore Computer Society (SCS) to provide career guidance in the field of cyber security
- A **Student Volunteer & Recognition Programme (SVRP)** with the Association of Information Security Professionals (AiSP)
- Annual **Cybersecurity Awards** with AiSP and 7 other professional and industry associations, to recognise *contributions* to the cyber security ecosystem
- A **Cyber Security Competency Framework (CSCF)** for cyber security professionals. CSCF lays out structured development pathways to drive capability development through targeted training, professional certification and career progression
- A **Smart Nation Scholarship (SNS)** with the government Technology Agency of Singapore (GovTech) and Info-communications Media Development Authority (IMDA) to develop and nurture tech leaders and talents in the Public Service. A total of 4 scholarships for cyber security were awarded in 2018

In addition, an example of a specific initiative of interest is the **Cyber Security Associates and Technologists (CSAT) Programme**[70]. This is a joint activity between the Cyber Security Agency of Singapore (CSA) and the Info-communications Media Development Authority of Singapore (IMDA), and is aimed at Singaporean citizens holding relevant diploma/degree qualifications in ICT, Engineering, Information Systems (IS), IS Security or related disciplines. The programme aims to train and up-skill fresh ICT professionals and mid-career professionals for Cyber Security job roles, offering a 12-month Associate Track (for those with 0-3 years' experience in ICT/networking roles) and a 6-month Technologist Track (for those with 3+ years' experience). Trainees will have opportunities to undergo on-the-job training programmes and participate in local and overseas attachments identified by 7 CSAT Training Partners (including Deloitte & Touche, KPMG, and PricewaterhouseCoopers).

South Africa

Speaking in March 2019, the Deputy Minister of Communications indicated that the government is working on long-term solutions to address the cyber security skills shortage[71]. Reference was made to initiatives around education and training, linked to recognition of cyber security roles and expertise:

- In terms of education, South Africa will have formal qualifications ranging from diplomas for school leavers through to graduate and post-graduate level degrees
- Additionally, reference was made to development of roles and responsibilities for the cyber security sector through the identification OFO (Organising Framework for Occupations) Codes

OFO coding is used as a skills-based classification system, and the South African Department of Higher Education and Training uses it as a means of monitoring skills demand and supply in the labour market. The 2017 version covers over 1,500 coded occupations, across different sectors of the workforce (e.g. from Managers and Professionals, through to areas such as Clerical Support and Machine Operators).

[70] CSA Singapore. 2019. Cyber Security Associates and Technologists Programme. 24 May 2019. https://www.csa.gov.sg/programmes/csat

[71] "South Africa to tackle cyber security shortage", BusinessTech, 27 March 2019. https://businesstech.co.za/news/technology/307362/south-africa-to-tackle-cyber-security-shortage/

Various technology occupations are identified, and as a specific example the OFO code 2017-252901 denotes an ICT Security Specialist.

The intention is to link various occupations to specific skills, identify further training needs, and then engage private service providers to develop cyber security training programmes. It will also define a framework of job descriptions relating to the cyber security careers necessary for the industry, accompanied by the educational requirements to ensure that candidates have the appropriate level of expertise to address the responsibilities of the role.

Thus, overall the aim is towards better understanding of cyber-related career paths, recognition of the skills that are needed to support them, and provision of education and training to increase the supply.

South Korea

A ***National Cybersecurity Strategy*** was released in April 2019[72]. It recognises the shortage of cyber security expertise in the face of increasing demand. The strategy indicates the intention for related action ("We will foster cyber security talent and continue to support the development of the cyber security industry"). Two of the specific Strategic Tasks within the document expand upon aspects relevant to improving cyber security capabilities. Specifically, under Task 4 (Build Foundations for Cyber security Industry Growth) there are sub-tasks relating to the specialist workforce:

Strengthen the competitiveness of the security workforce and technology:

- Equip cyber security personnel with world-class expertise and competitiveness to respond to sophisticated cyber security threats
- Strengthen customised personnel development programmes to provide businesses, government, the military and society with a cyber workforce equipped with diverse capabilities
- Devise measures to improve cyber security expertise and recruit talented personnel

Meanwhile, under Task 5 (Foster a Cyber Security Culture), there are points relating to raising the capabilities of the more general user population:

Raise cyber security awareness and strengthen cyber security practice:

- Develop and distribute basic rules of cyber security so people can realise the importance of cyber security and easily put such rules into practice in their daily lives
- Develop and employ education programmes for cyber ethics and security customised to specific sectors of society, such as students, government officials, military personnel, and company employees
- Strengthen corporate social responsibility of businesses to protect cyber space and maintain an appropriate level of security in their products and services

However, the Strategy does not go beyond these high-level aspirations, and makes reference to the *National Cybersecurity Basic Plan* and the *National Cybersecurity Implementation Plan* as future initiatives that will give shape to the actual implementation

[72] National Security Office. 2019. *National Cybersecurity Strategy*. Republic of Korea, April 2019. Publication Registration Number 12-1025000-000003-01. https://www.msit.go.kr/cms/www/work/ict/__icsFiles/afieldfile/2019/04/03/국가사이버안보전략(영문)_0403.pdf

United States

The **Executive Order on America's Cybersecurity Workforce**[73] was issued in May 2019, which recognises the need to enhance the workforce mobility of cyber security practitioners, indicating that government policy must facilitate the seamless movement of practitioners between public and private sectors. It cites a requirement for "innovative approaches" to improve access to training and the need to enhance opportunities around work-based learning, apprenticeships, and blended learning, and applying to both new entrants in the workforce and workers at advanced stages in their careers.

In relation to the federal workforce:

- Establishment of a cyber security rotational assignment programme for the Federal cyber security workforce, to enable a knowledge transfer and a development programme for cyber security practitioners. This will include training and peer mentoring, with the Department of Homeland Security sharing cyber security experts with other agencies and taking staff from other agencies to work in DHS. The NICE Framework will be used as the basis for identifying and describing the cyber security skill requirements for programme participants

In the more general workforce context:

- A national Call to Action to highlight, and mobilise public and private sector resources to address cyber security workforce needs
- Align education and training with employers' cyber security workforce needs
- Encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts

There is also the proposal for 2 annual initiatives to recognise cyber security talent:

- A President's Cup Cyber Security Competition for Federal civilian and military employees, that aims to recognise the best government practitioners and teams in offensive and defensive cyber security disciplines
- A Presidential Cyber Security Education Award for school educators in cyber security and related subjects, with awards to one elementary and one secondary level educator per year

European Network and Information Security Agency (ENISA)

ENISA has developed a National Cyber Security Strategy Good Practice Guide, the most recent version of which is from 2016[74]. This includes a number of Key Performance Indicators that are intended to allow policy makers to track the success of the implementation of strategic objectives. Two sets of these indicators are broadly related to the area of cyber skills, and are presented below, directly as expressed in the guidance:

- **Raise user awareness:** Indicators for the performance of user awareness measures are the number of campaigns and similar events arranged by public and private entities. These measures should focus on areas, in which a lack of awareness or knowledge has been identified
  - The existence of measures to identify target areas for awareness raising

[73] Trump, D.J. 2019. *Executive Order on America's Cybersecurity Workforce*. The White House, 2 May 2019. https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

[74] ENISA. 2016. *NCSS Good Practice Guide - Designing and Implementing National Cyber Security Strategies*. 14 November 2016. https://www.enisa.europa.eu/publications/ncss-good-practice-guide

  - The areas/topics covered by awareness raising campaigns (e.g. end-user, children, Critical Information Infrastructure Protection)
  - The number of public awareness raising events (e.g. conferences, workshops)
  - The number of corporate in-house awareness raising measures

- **Strengthen training and educational programmes:** Education about information security as well as skilled personnel in key positions is imperative to increase the overall level of national cyber security. Typical KPIs include:

  - The number of cyber security courses established
  - The number of annual information security events (e.g. hacking contests or hackathons)
  - The number of accredited or certified personnel in the private and public sector

The following table summarises the status of the implementation of these aspects within the EU Member States and EFTA countries encompassed by the report at the time of its publication in late 2016. While the majority are demonstrating attention to both areas, the picture was clearly not consistent across the countries assessed.

User awareness and education initiatives in EU Member States and EFTA countries

Country	Raise user awareness	Strengthen training and educational programmes
Austria		3
Belgium	3	3
Bulgaria	3	3
Croatia		
Denmark	3	3
Estonia	3	3
Finland	3	3
France	3	3
Greece	3	
Hungary		3
Ireland		
Luxembourg	3	3
Malta	3	3
Slovenia	3	3
Spain	3	3
Sweden		
Switzerland	3	3

An interactive online map at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map lists 8 additional countries addressing both areas (Cyprus, Latvia, Lithuania, Norway Poland, Romania, the Slovak Republic, and the UK). Meanwhile, the Czech Republic addresses only the awareness category (which is now titled Citizen's Awareness in the latest materials), and the

Netherlands only addresses training and education programmes. None of the gaps indicated in the table have yet been filled.

Lessons from the international landscape

The clear and common finding is there are national cyber security strategies highlighting the need to attend to reskilling/upskilling within the current workforce, alongside to grow the pipeline of future talent via education and research. There are no major revelations in terms of the ideas and initiatives being pursued from one country to another (although some points of interest were highlighted in the summaries), and in most cases too early to see any impact (the notable exception here being Israel, which can be regarded as a beacon in terms of the influence its approach appears to have had upon others).

There are nonetheless some useful points that can be highlighted, drawing upon some of the specifics indicated above:

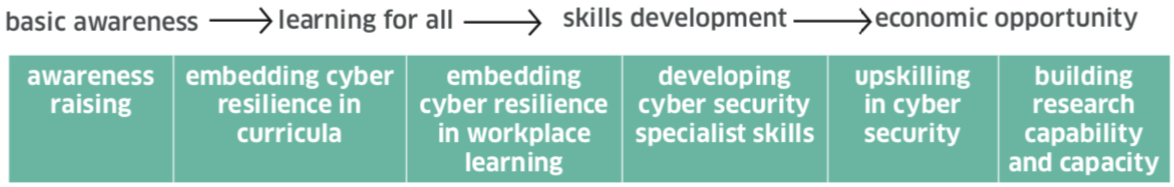
- A key theme that is apparent from various initiatives is the attempt to align efforts from education, research, and training through to the workforce. This coordination is typically achieved through the over-arching context of a national cyber security strategy
- Efforts are being made to support growth of the cyber security talent pool. This includes:
  - Schemes to encourage and enable individuals to engage with cyber security, particularly at earlier stages and recognising that the target audience is diverse and extends beyond computing topics
  - Support for the establishment of new education and training programmes. This can include both financial support (in terms of priming programme development and offering scholarships).
  - Routes to enable individuals with relevant skills to further develop towards specialisation in cyber security (as with the Singaporean CSAT programme)
- Enabling a better understanding of cyber careers and routes into the profession. Provisions such as a the AustCyber dashboards have potential to be of benefit in this context to raise awareness, while the formal definition of occupations/roles (as seen in South Africa) helps to target efforts towards those that are needed
- It is desirable to ensure recognition of existing professionals, via awards for those holding skills and supporting others to acquire them. Linking back to the earlier evidence of workload and stress, any initiatives that help individuals to feel valued are likely to be beneficial
- Initiatives need to be targeted across the board, from school education, through HE and into CPD contexts. There is not a single route into cyber security, and the skills shortfall can be addressed by harnessing both new entrants and career changers, plus recognising the need for existing professionals to develop and maintain their skills
- It is important to recognise the need to support the general workforce and specialist cyber skills. Effective citizen awareness initiatives have the potential to reduce the challenges that specialists then need to address as a result of staff within their own workplace

Interestingly, much of this is already encapsulated within UK strategy such as ***Scotland's Learning & Skills Action Plan for Cyber Resilience***[75] and ***the UK's Initial National Cyber Security Skills***

[75] Scottish government. 2018. Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland. Learning & Skills Action Plan for Cyber Resilience 2018-20. The Scottish government, March 2018. https://www.gov.scot/publications/learning-skills-action-plan-cyber-resilience-2018-20/

Strategy[76]. The fundamental principle of this plan is that cyber resilience (and the opportunities arising from it) will not be achieved unless it is embedded across the learning and skills system (as illustrated by the continuum in Figure 11).

Figure 11: Continuum of cyber resilience learning and skills


basic awareness
learning for all
skills development
economic opportunity
awareness raising
embedding cyber resilience in curricula
embedding cyber resilience in workplace learning
developing cyber security specialist skills
upskilling in cyber security
building research capability and capacity

The plan identifies 4 resulting aims as below (as well as 37 underlying actions for addressing them):

- Increase people’s cyber resilience through awareness raising and engagement
- Explicitly embed cyber resilience throughout our education and lifelong learning system
- Increase people’s cyber resilience at work
- Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland

The resulting initiative represents an integrated approach, with collaboration between government, academia and industry, with the potential for positive effects across the identified continuum.

[76] See https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary,

Appendix B: training provider interviews topic guide

Introduction

- This is part of a wider programme of research on cyber security skills in the UK. These conversations with training providers are about understanding the training products and services market. Primarily (FOR CONTEXT AND NO NEED TO READ OUT):
    - The types and categories of things on offer
    - Where the is demand from and what types/content of training they want
    - Where the demand is heading in the next 2 to 5 years
    - The scale and scalability of their offer, and the challenges around this
- MUST READ OUT: *All responses are confidential and anonymous. DCMS won't know who has taken part and will get an anonymised report pulling out the key findings across all interviews.*
- MUST GET PERMISSION TO DIGITALLY RECORD FOR ANALYSIS (AND EXPLAIN WE WON'T ATTRIBUTE) AND TO SHARE THIS RECORDING WITH RESEARCH PARTNER: *We're doing this research with a partner organisation (Perspective Economics/Ipsos MORI) and would like to share the recording with them. They and we will securely destroy it after the research is complete. Can I just check this is okay with you?*

Training offer (c.15 minutes)

WARM UP: Tell me a bit about your organisation and your role within it.

What kinds of products and services do you currently offer? How would you categorise the product or service lines your offer?

- What's the best way of categorising it? By training content, delivery channel, who it's targeted at etc.?
- What types of organisations or individuals use their products and services?
- Do they focus on a particular kind of training or do everything?
- What is most in demand right now? What type/categories? Anything less in demand/less needed than before? Why do they think this is?

How do clients find you?

- Do they find them through word-of-mouth, internet searching, direct marketing etc.?

Where does your business fit into the rest of the cyber skills training market?

- What is the industry like? Lots of small providers offering niche products/services, or a few all-round providers offering a range of solutions?
- What is their business model? What made them go with this approach? How is this similar/different to other providers?
- What kinds of other models/provision are out there?

Does your training lead to any qualifications?

- Which qualifications?
- How much does this matter to clients? What difference would it make if they didn't emerge with a qualification? What kinds of clients does this appear more/less to?

How do you see demand changing over the next 2 to 5 years?

- Any particular types of training increasing in demand? Move to products or services? Move towards/away from tailored training? Need for cheaper/broader training? Demand from new types of businesses (e.g. size and sector)?

- What innovation is taking place in the market? New delivery channels/products/services? Where is the demand coming from for these new things?
- Are they/have they made any changes in anticipation, e.g. new courses/ products/services? Are they planning to do this?

Clients and demand (c.15m)

How would you describe your "typical" clients?

- Do you provide training mainly for organisations or do you also provide training to individuals who come to you directly?
- Geographical locations – do they only work locally or more widely? How feasible is it to go wider than this?
- Focus on particular sizes of clients or industry sectors, e.g. financial services? Do different sizes/sectors have different needs?
- Do certain types of clients have similar needs or is it unique for each client?
- How stable has this been? Have your clients changed over the past few years? What do you expect over the next 2 to 5 years?

How aware are clients of their training needs?

- How informed are client organisations and individuals within client organisations when choosing training products and services?
- Do clients know what kind of training they want from the start, or does the training provider have to suggest what kind of training the client might want/need?
- If you are dealing with individuals directly, how informed are they when choosing training products and services?
- Do they provide a fixed "off-the-shelf" product or service, or whether they have tailored offers for each client?

How big is your demand currently?

- Probe on the scale of their offer i.e. what volume of clients they can/do service.

How scalable is your offer? How easily could you expand to serve more clients?

- How easily or quickly do they think they could do this?
- Probe on constraints/challenges to scaling up (e.g. staff numbers, their own skills shortages/gaps, investment/access to finance)
- What actions would they need to take to grow supply?

Other issues – partnerships, initiatives and diversity (c.10m)

We will know what to probe here based on the company descriptions in the sample.

Do you have any partnerships (formal or informal) with academic institutions or other businesses?

IF YES, PROBE:

- What are the most important impacts they think come out of this partnership?
- Does this help to provide a route into industry for training recipients? Do they partner with any businesses to place the trained individuals in jobs/work experience?
- Are they collaborating with businesses to offer them any tailored products or services?
- How does it help tackle skills shortages? Does it help the training provider better align their training with industry needs?

Are you involved in any government-sponsored schemes for cyber skills and training, such as Cyber First, Cyber Discovery or the Cyber Skills Immediate Impact Fund?

IF YES, PROBE:

- What do they feel has changed as a result of the scheme, e.g. have they increased provision of products/services or do they offer a new product/services?

Do your training products/services have any focus on improving diversity and accessibility in the sector?

IF YES, PROBE:

- How does this work? Have you moved away from traditional learning methods to support this? What has worked well?
- How has it broadened participation? Any examples of where it has led to people considering cyber security as a career where they might not have before?

Wrap-up

- Is there anything that we haven't discussed that you would like to raise?
- READ OUT: *Ipsos MORI and Perspective Economics are carrying out further research including a telephone survey as part of this study on cyber security skills. Would you be happy for Ipsos MORI or Perspective Economics to share your contact details, so that we can recontact you if needed for the next stages of the project? There would be no obligation for you to take part.*
- GET DETAILS FOR £50 THANK YOU INCENTIVE (AS CHEQUE EITHER MADE OUT TO CHARITY OR TO PARTICIPANT)

Appendix C: categorisation of training products and services (from strand 2)

Type of Training	Awareness / Board - Level	Introductory / Principles of Cyber Security	Introductory / Application Focus	Introductory (Bootcamp)	Intermediate / Advanced Courses	Online CPD (Ongoing)
Level of Experience:	Limited – can be provided at all levels.		Can be novice (no experience at all) to basic/intermediate (some background in networking/IT)		Some background in IT / cyber security typically sought (applied experience or CompTIA Network+ etc)	Typically application / technique focused. Need to demonstrate experience.
Time Commitment	Low (1-2 days)	Step up from awareness, but typically 2-5 days.	With application focus (i.e. a particular piece of software/technique), can be delivered within 1-4 weeks.	Core training delivered typically within an 8-12 week period, with cohort support for longer (9-12 months) period to find work opportunities. Can be augmented with prior online training.	Depends on course undertaken, but intermediate / practitioner courses can take 5-10 days (e.g. CISSP)	Varied (users can select modules for completion in own time).
Training Platform	Can be a mix of online theory, with time committed for board workshops	Can be online/classroom based.	Typically uses online resources, but may require some F2F training and discussion. Can be online only (e.g. HackerHouse) but typically includes F2F interaction.		Can become more classroom focused (with some access to online platforms) Can also do online courses/ book exams.	Can be online/classroom based. Subject to experience, often online only.
Accreditations / Qualifications?	No – but may enable organisational level accreditations / demonstrate commitment to good practice	Limited (basic)	More focus on certification / pass rate with respect to a single piece of software (e.g. IBM QRadar)	Mixed. Training can be aligned to enabling completion of accreditation (CompTIA Network+/Security+, CISMP etc) or without accreditation/exam, but demonstration of skills-set (through meeting employers, completion of online labs)	Typically accreditation focused (exam at end). Customer knows end outcome.	Can be gamified / platform certificates. Not necessarily formal qualifications, but often recognised in marketplace e.g. AWS Certified Security training.
Typical Entrants:	Board-level / staff	Open	Can be from any background, but need to demonstrate basic aptitude / willingness to be involved within the sector. Recognition that entrance route must accommodate entrant requirements where diversity/inclusion is crucial e.g. 9-5pm can be challenging		Intermediate-Level / those working within sector or IT aligned	No formal barriers to entry, but prerequisite knowledge advised
Typical Financial Model:	Typically B2B (reflected in a business' internal investment in cyber security)	Limited/low cost. Can either be B2B (classroom setting) or online courses often free/low cost.	CSIIF projects currently receiving match funding. Stakeholder consultation indicating that industry is willing to engage and support financially; however, government funding needed to adequately finance projects and ensure diversity.		Privately funded – could be by individual or business. Costs for CISSP might vary from between £500 (for exam only) to £3,000 (incl. classroom training)	Can be low cost (online training at scale). Some providers B2B (e.g. Immersive Labs for Digital Academy model), others with individual and business pricing.
Example Providers:	QA, Xyone Cyber, The Defence Works	Some private (incl. GCHQ accredited) also OU FutureLearn	SaluteMyJob, Worcester Community SOC	CompTIA (CyberReady), QA with Women Tech Jobs	BlueScreen IT, Crucial Academy	Immersive Labs, CompTIA, QA – but also A Cloud Guru, Udemy, Udacity, Linux Academy etc.

Appendix D: quantitative questionnaire

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

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

Introduction

Is this the head office for [SAMPLE S_CONAME]?

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

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

SAMPLE S_FREENUMTEXT

SAMPLE S_RESPTEXTSUB

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

ADD IF NECESSARY:

- The survey will help inform government policy on how it can best help organisations like yours to address their skills and recruitment needs.
- As a thank you for taking part, we can send you last year's report and infographics, and a government help card with the latest official cyber security guidance for organisations like yours. These would get emailed to you as soon as you complete the survey.

ADD DEFINITION OF CYBER SECURITY IF NECESSARY:

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

REASSURANCES IF NECESSARY:

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

Reassurance email

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

- 170 refused – outsources cyber security
- 171 soft refusal
- 172 refused – no cyber security issues/problems
- 173 refused – think survey is not genuine
- 174 refused – company no-name policy
- 175 refused – cyber security is commercially confidential

- 180 – wrong direct line
- 181 – duplicate business
- 201 ineligible – sole trader at SIZEA
- 247 ineligible – no computer, website or online use
- 249 ineligible – sole trader at intro

Consent

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

If you would like to read the privacy policy before we continue, I can give you the link. If you're happy to proceed we'll continue.
ADD IF NECESSARY: You can access the privacy policy on our website at: https://ipsos.uk/3993p.

SINGLE CODE
Yes
No
CODE 2 CLOSES SURVEY

ASK IF CYBER SECTOR BUSINESS (SAMPLE S_TYPE=3)
Q1y.CONSENTC
Your business may have taken part in an Ipsos MORI survey for DCMS in May or June 2019, which was about understanding the UK cyber sector. We can reuse your answers from that survey in this one to make it much shorter. To do this, we would have to match your business details across both surveys. Are you happy for us to do this?
INTERVIEWER NOTE: IF THEY SAY NO, REITERATE THAT THIS IS SO WE CAN AVOID ASKING THEM TO REPEAT THEIR ANSWERS IN THE PREVIOUS SURVEY.

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

DUMMY VARIABLE NOT ASKED
Q1z.CONSENTCDUM

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

Organisational profile

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

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

SINGLE CODE
Mainly seeking to make a profit
A social enterprise
A charity or voluntary sector organisation

A government-financed body or public sector organisation
DO NOT READ OUT: Don’t know

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

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

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

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

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

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

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

DUMMY VARIABLE NOT ASKED
Q3a.SIZE

Which of these best represents the number of employees, volunteers and trustees working in your organisation, including yourself?

SINGLE CODE, MERGE RESPONSES FROM SAMPLE S_SECTORALSIZE, SIZEA AND SIZEB
Under 10
10 to 49
50 to 249
250 to 999
1,000 or more
Don't know

ASK IF NOT PUBLIC SECTOR, INCOME NOT ALREADY AVAILABLE, AND NOT SKIPPING QUESTIONS (SAMPLE S_INCOMEBAND=_06, TYPEXDUM NOT CODE 3 AND CONSENTCDUM NOT CODE 1)
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)
DO NOT READ OUT: Don't know
DO NOT READ OUT: Refused

ASK IF DON'T KNOW NUMERIC TURNOVER OF ORGANISATION (SALESA CODE DK OR REF)
Q5.SALESB
Which of these best represents the [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

SINGLE CODE
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

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?

SINGLE CODE, MERGE RESPONSES FROM SAMPLE S_SECTORALSALES, SALESA AND SALESB
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

Q6.DEFINE DELETED POST-PILOT IN 2018

Outsourcing

ASK IF NOT CYBER SECTOR (TYPXDUM NOT CODE 4)
Q7.OUTSOURCE

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

SINGLE CODE
Yes
No
Don't know

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

Q8.HOWMUCH DELETED IN 2019

Q9.REASONOUT DELETED IN 2019

Q10.INVESTOUT DELETED POST-PILOT IN 2018

Q11.INVESTOUTB DELETED POST-PILOT IN 2018

Q12.OUTVALUES DELETED POST-PILOT IN 2018

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

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP i LAST

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

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

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

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP g LAST

a. Designing secure networks, systems and application architectures
b. Penetration testing
c. Using cyber threat intelligence tools or platforms

d. Carrying out forensic analysis of cyber security breaches
e. Interpreting malicious code, or the results shown after running anti-virus software
f. Using tools to monitor user activity

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

Q15.DEALINGOUT DELETED IN 2019

Q16.PERFORMOUT DELETED POST-PILOT IN 2018

Workforce size

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

ASK IF NOT CYBER SECTOR (TYPXDUM NOT CODE 4)
Q16a.TITLE
What is your job title, and the name of any team or department you work in?
PROMPT TO CODE, INCLUDING IF RELATED DIRECTLY TO CYBER SECURITY OR NOT
CODE TO BOTH A JOB TITLE AND A TEAM/DEPARTMENT

SINGLE CODE PER BOLD HEADING
Job title
Related to cyber security/security
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)
Director of Security
Head of Cyber Security/Information Security
Other cyber security role WRITE IN

Not related to cyber security – senior
Business owner
Chief Executive (CEO)/Managing Director (MD)
Trustee/treasurer/on trustee board
Other senior management role (e.g. director) WRITE IN

Not related to cyber security – non-senior
General manager (not a director/trustee)
PA/secretary/administrator
Other non-senior role WRITE IN

Team or department
Cyber security/information security
Compliance/legal
Finance/accounts
Information governance
IT/service desk
Management board/senior management/trustees
Other team or department WRITE IN
DO NOT READ OUT: No specific team or department

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

WRITE IN RANGE 1 TO [SIZEA OR TOP END OF SIZEB] OR [99 IF SIZE=DK]
IF MICRO (SIZEA CODE<10 OR SIZEB CODE 1): (SOFT CHECK IF >3)

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

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

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

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

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

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

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

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

SINGLE CODE, MERGE RESPONSES FROM SAMPLE S_SECTORALCYBERSIZE, S_SECTORALCYBERSIZEB, CYBERSIZE AND CYBERSIZEB, AND SIZEA IF SOLE TRADER
1 to 4
5 to 9
10 to 29
30 to 49
50 to 249
250 to 499
500 to 999
1,000 or more
Don't know

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

READ OUT
IF ONE PERSON (TEAM=1): INTERVIEWER NOTE: CODE “1” AT RELEVANT RESPONSE

ASK AS A GRID

a. Recruited or joined from a **non**-cyber security related previous role
b. Recruited or joined 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 TO TEAM OR [99 IF TEAM=DK] FOR EACH STATEMENT
HARD CHECK IF TOTAL ACROSS STATEMENTS >TEAM
DO NOT READ OUT: Don’t know

READ OUT IF CYBER SECTOR AND NOT SOLE TRADER (CYBERSIZEDUM≠1)
Now I would like to ask some questions about the people working in cyber security roles **within** your organisation, including you.
IF SKIPPING QUESTIONS (CONSENTCDUM CODE 1): In the previous survey you took part in, we recorded that this was [CYBERSIZEDUM OR CYBERSIZEBDUM] employees.

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
Q18b.PATHWAYNUM
IF SOLE TRADER (CYBERSIZEDUM=1): Did you enter this role in any of the following ways?
IF NOT SOLE TRADER (CYBERSIZEDUM≠1): Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, including you, how many entered this role in each of the following ways?
READ OUT

ASK AS A GRID

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

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

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

ASK AS A GRID

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

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

Workforce diversity

Q19.DIVERSITYA DELETED IN 2019

ASK IF SMALL CYBER SECTOR (CYBERSIZEBDUM CODES 1 TO 3)
Q19a.FEMALENUM

Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, how many are female?
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

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

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

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

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

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

Q20.DIVERSITYB DELETED IN 2019

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

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

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

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

ASK IF LARGE CYBER SECTOR (TYPXDUM CODE 4 AND CYBERSIZEBDUM CODES 4 TO DK)
Q20c.BAMEPER

Of all the [CYBERSIZEDUM OR CYBERSIZEBDUM] employees working in cyber security roles, roughly what proportion are from ethnic minority backgrounds?
PROBE FULLY (I.E. UNTIL YOU REACH THE RIGHT ANSWER)
ADD IF NECESSARY: The answers won't be linked to your business. They will be aggregated across all interviews, to help us measure diversity across the whole cyber security sector.

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

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

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

Q21.DIVERSITYDUM DELETED IN 2019

Workforce qualifications

ASK IF CYBER SECTOR (TYPEXDUM CODE 4)
Q22.QUALS
Do you or any other employees in cyber security roles have, or are they working towards, any cyber security-related qualifications or certified training?
DO NOT READ OUT

SINGLE CODE
Yes
No
Don't know

ASK IF QUALIFICATIONS (QUALS CODE 1)
Q23.WHICHQUALS
Which of the following types of qualifications or certified training do you or other employees have, or are they working towards?
READ OUT

MULTICODE
A specialist higher education qualification (e.g. a degree) related to cyber security
A general computer science, information systems or IT higher education qualification
A cyber security apprenticeship
Any other apprenticeship
Any other technical qualifications or certified training related to cyber security

SINGLE CODE
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these

ASK IF OTHER QUALIFICATIONS (WHICHQUALS CODE 5)
Q24.WHICHCERT
Which other technical qualifications or certified training do you or other employees have, or are they working towards?
DO NOT READ OUT
PROBE FULLY, I.E. "ANYTHING ELSE?"

MULTICODE
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)
Cisco CCNA certification
CREST-approved training
Cyber Essentials certification
CyberSec First Responder
CompTIA Security+
Digital Cyber Academy/Immersive Labs training
Foundation Certificate in Cyber Security
GDPR-specific certificates
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)
Microsoft Certified Professional (MCP)
PCI DSS training
Practitioner Certificate in Information Assurance Architecture
Security & Information Risk Advisor (SIRA, certified by IISP)
Other WRITE IN
SINGLE CODE
Don't know

Q25.SENIORITY DELETED IN 2019

Formal versus informal cyber security roles

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
Q26.FORMAL
Is cyber security a formal part of your job description, or do you cover this role informally?
DO NOT READ OUT

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

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
Q27.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

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

Skills and knowledge of responsible individual or team

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

RANDOMISE STATEMENT ORDER BUT KEEP f AND g TOGETHER

a. IF CYBER SECTOR (TYPEXDUM CODE 4): Soft skills, such as oral or written communication skills and team working skills
b. **STATEMENT DELETED POST-PILOT IN 2018**
c. **STATEMENT DELETED IN 2019**
d. IF CYBER SECTOR (TYPEXDUM CODE 4): Understanding the legal or compliance issues affecting cyber security, such as data protection
e. **STATEMENT DELETED IN 2019**
f. IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4): **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
g. IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4): **High-level technical skills**, which could include things like:
   - security engineering or architecture
   - penetration testing
   - using threat intelligence tools
   - forensic analysis
   - interpreting malicious code
   - or using tools to monitor user activity
h. IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4): **Incident response skills**, which could include things like writing an incident response plan, incident management and recovery from cyber security breaches

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

SCRIPT TO ROTATE ORDER OF TECHNICAL, MANAGERIAL AND KNOWLEDGE

ASK IF NOT CYBER SECTOR (TYPEXDUM NOT CODE 4)
Q29.TECHNICAL

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

RANDOMISE STATEMENT ORDER

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

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

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

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

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

RANDOMISE STATEMENT ORDER

a. ASK HALF THE SAMPLE (HALF A): Communicating cyber security risks effectively to directors, trustees or senior management

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

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

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

RANDOMISE STATEMENT ORDER

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

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

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

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

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

RANDOMISE STATEMENT ORDER

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

g. **STATEMENT DELETED POST-PILOT IN 2018**
h. The staffing needs of cyber security within your organisation

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

Q33.DIRECTDUM DELETED IN 2019

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

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

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

Training and upskilling

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

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

Q35.VALUE DELETED POST-PILOT IN 2018

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

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

ASK ALL
Q36.NEEDS
In the last 12 months, has anyone undertaken a formal analysis of your organisation’s cyber security skills or training needs?

DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

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

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

Q37.SOUGHT DELETED IN 2019

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

SINGLE CODE
Yes
No
Don’t know

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

ASK AS A GRID
RANDOMISE STATEMENT ORDER BUT KEEP a AND b, AS WELL AS c AND d TOGETHER

a. IF LOOP A: Introductory training for new joiners or graduates entering cyber security roles
b. IF LOOP A: Continuing professional development training for staff who are not new joiners
c. IF LOOP B: Specific training sessions devoted to cyber security
d. IF LOOP B: Broader training sessions, for example on GDPR, where cyber security was covered
e. IF LOOP B: Training specifically for directors, senior managers or trustees
f. Developed internally within the organisation
g. Developed externally outside the organisation
h. Mandatory training

SINGLE CODE
Yes
No
Don’t know

Q38.BARRIERS DELETED IN 2019

Q39.MODE DELETED IN 2019

Q40.TRAINER DELETED POST-PILOT IN 2018

Q41.TRAINERDUM DELETED POST-PILOT IN 2018

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

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

Recruitment and retention

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

ASK IF CYBER SECTOR (TYPEXDUM CODE 4)
Q43.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 skills needs in your organisation? This includes any current vacancies you may have.
DO NOT READ OUT

SINGLE CODE
Yes
No
Don’t know

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

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

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

Other
Ads in newspapers or magazines
Asking individuals to apply directly
Headhunting (but not through recruitment agency)
Recruiting from elsewhere in organisation
Recruiting from universities/graduate placements
Word-of-mouth/industry networks/recommendations
Other WRITE IN

SINGLE CODE
Don’t know

ASK IF TRIED TO RECRUIT (RECRUIT CODE 1)
Q45.VACANCIES
How many vacancies have you had in cyber security roles within the last 3 or so years?
PROBE FOR BEST ESTIMATE BEFORE CODING DK

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

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

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

ASK IF HARD-TO-RECRUIT VACANCIES (HARD>0)
Q46b.HARDROLE
IF ONE VACANCY (VACANCIES=1): What specific role or occupation was this hard-to-fill vacancy in?
IF MORE THAN ONE VACANCY (VACANCIES>1 OR DK): What specific roles or occupations were these hard-to-fill vacancies in?
PROMPT TO CODE
READ OUT TEXT IN BOLD BEFORE CODING “OTHER”. ADD ADDITIONAL DESCRIPTIONS IF NECESSARY.
INTERVIEWER NOTE: IF JUST “ANALYST” OR “CONSULTANT”, PROMPT WITH BOLD TEXT BEFORE CODING “OTHER”.

MULTICODE RESPONSES UNDER THE UNDERLINED HEADINGS UP TO HARD
<u>Generalist roles</u>
Generalist cyber security role
Generalist IT role
Generalist sales role

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

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

MULTICODE UP TO HARD
Apprentices
Entry-level staff or graduates

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

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

MULTICODE RESPONSES UNDER THE BOLD HEADINGS
Offer not good enough
Job is difficult/challenging
Low pay or benefits 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/knowledge
Lack of qualifications
Lack of work experience

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

SINGLE CODE
Don't know

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

ASK AS A GRID

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

SINGLE CODE
Yes
No
Don't know

Recontact

ASK ALL
Q48.RECON
Would you be happy to take part in a more bespoke interview with Ipsos MORI in autumn 2019, to further explore some of the issues from this survey? This interview would be more of a conversation on the issues relevant to your organisation, rather than a structured questionnaire.

ADD IF NECESSARY: The interviews would last no longer than 45 minutes and those taking part would be offered a £50 cheque or a donation to the charity of their choice.

SINGLE CODE
Yes
No

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

SINGLE CODE
Yes
No

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

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

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

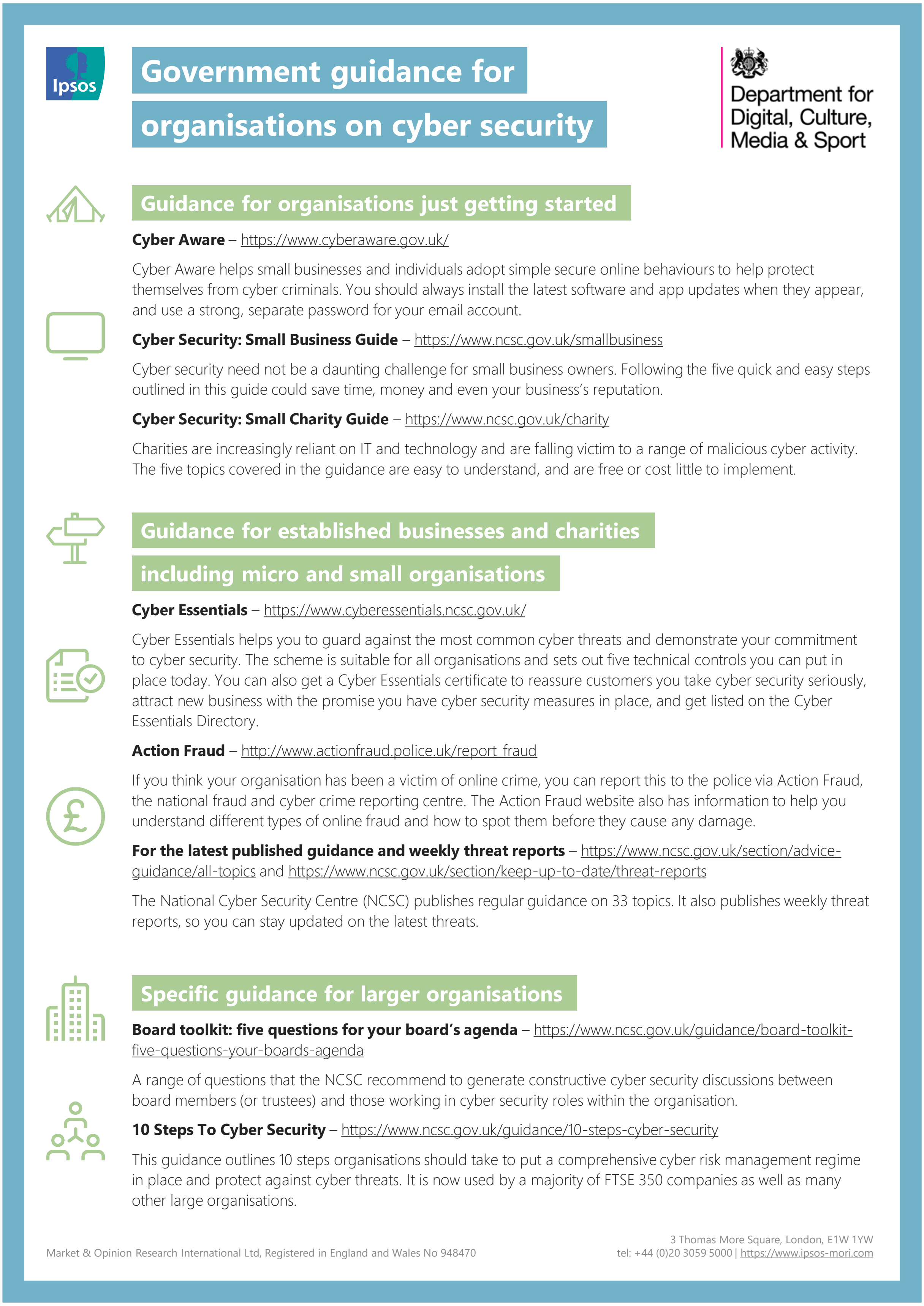
GDPR privacy policy

READ OUT TO ALL
Thank you for taking the time to participate. You can access the privacy policy on our website at: https://ipsos.uk/3993p. This explains the purposes for processing your personal data, as well as your rights under data protection regulations to:

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

CLOSE SURVEY

Appendix E: government help card offered to survey respondents



Ipsos

Government guidance for organisations on cyber security

Department for Digital, Culture, Media & Sport

Guidance for organisations just getting started

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

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

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

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

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

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

Guidance for established businesses and charities including micro and small organisations

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

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

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

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

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

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

Specific guidance for larger organisations

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

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

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

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

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

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

Appendix F: large organisation and cyber sector businesses topic guides

Large organisations

Introduction (2-3 minutes)

- Introduce self and Ipsos MORI: independent research organisation (i.e. independent of government).
- Thank participant for taking part and explain that we are speaking with them to learn more about the cyber skills labour market, to help inform future government policy.
- Interview should last about 45 minutes.
- Incentives: as a thank you, £50 will be paid to the participant or a charity of their choice.
- MUST GET PERMISSION TO DIGITALLY RECORD FOR ANALYSIS: Explain recordings will be securely destroyed after the research is complete. If necessary, explain that they will be stored securely and only the research team at Ipsos MORI will have access to these.
- MUST READ OUT AFTER STARTED RECORDING: In any published reports, the findings from this interview will be anonymised and presented at an aggregated level. Large organisations will not be identifiable. Participation is voluntary and you can change your mind at any time. However, the sample of large organisations we are interviewing is relatively small, at around 15 organisations. This means that the team in DCMS that provided the contacts for these organisations may be able to identify the ones that have taken part. Can I confirm you are happy to take part on this basis?
- If you would like to read the privacy policy before we continue, I can give you the link. If you're happy to proceed we'll continue. ADD IF NECESSARY: You can access the privacy policy on our website at: https://ipsos.uk/3993p.

Context (c.5 minutes)

- Tell me a bit about your organisation and your role within it. How long have you been with the organisation?
- What are your day-to-day tasks? PROMPT ON CYBER SECURITY RESPONSIBILITIES.
- Who else makes decisions around cyber security/cyber security training and recruitment within your organisation? What is your role in this?
- Including yourself, how many employees work in your organisation across the UK as a whole? And how many, including yourself, are directly involved in managing or running your organisation’s cyber security? RECORD ANSWERS. IF SIGNIFICANT NUMBERS (5+): How many people working on cyber security have technical roles and how many have non-technical roles (for instance cyber security training)?
- How many of your cyber security staff are EU nationals?
- READ OUT: How well, if at all, would you say your organisation’s directors or senior managers understand the cyber security risks facing your organisation? *Very well, Fairly well, Not very well, Not at all well.* RECORD ANSWERS. What implications does this have? And how important do directors and senior managers think cyber security risks are? What sort of priority does cyber security have?
- What are the career backgrounds of employees working in cyber security roles? What is your career background? Did any join from non-cyber security roles or non-technical roles? What led to them working in a cyber role? IF ANY STAFF HAVE NON-TECHNICAL ROLES, PROBE ON DIFFERENCES IN BACKGROUNDS.

Skills gaps (c.7 minutes)

Current skills

- In what ways does your organisation support employees in cyber roles? PROBE ON HIRING STRATEGY, MENTORING, WELFARE INITIATIVES.

- To what extent is there a shortage of cyber skills in your organisation? PROBE ON BASIC SKILLS, HIGHER-LEVEL SKILLS AND SOFT SKILLS, AS WELL AS SENIORITY. What impact is exiting the EU likely to have on your organisation's cyber skills now and in the future?
- READ OUT: How well, if at all, would you say your organisation's directors or senior managers understand the staffing needs of cyber security within your organisation? *Very well, Fairly well, Not very well, Not at all well.* RECORD ANSWERS. What makes you say this? And what importance do directors/senior managers give to cyber security staffing?
- What steps does your organisation take to tackle skills gaps? Which cyber skillsets or experience is your organisation looking to acquire?
- To what extent do your cyber teams have to take on multiple roles or adapt their working patterns to address skills shortages? What support is provided to teams in these cases?
- What particular challenges do you think large organisations in terms of cyber skills? PROBE WHETHER PARTICULAR SKILLS NEEDS/PROCEDURES/SYSTEMS UNIQUE TO LARGE ORGANISATIONS.

Upcoming skills gaps

- Looking to the future, how do you think the needs of the organisation in relation to cyber security might change in the next 5 years? What implications will this have for cyber skills? Are gaps in cyber skills likely to get better or worse? Why is that?
- What potential impact might this have on your organisation? What steps is your organisation taking in relation to this? PROBE ON WHETHER UNIQUE TO LARGE ORGANISATIONS IN ANY WAY.

Role of government

- What role does the government have in addressing cyber skills gaps in organisations like yours? What steps should it be taking?

Training (c.10 minutes)

- What are your organisation's needs in respect of training and upskilling in cyber security? What parts of the organisation are most urgently in need of training or awareness raising? PROBE ON DIFFERENT TRAINING NEEDS FOR CYBER TEAMS, SENIOR MANAGEMENT AND WIDER STAFF.
- READ OUT: In the last 12 months, has anyone undertaken a formal analysis of your organisation's cyber security skills or training needs? RECORD ANSWERS. What did this involve? Who undertook this analysis and why? PROBE SEPARATELY ON SKILLS AND TRAINING. IF THERE ARE DIFFERENCES, ASK WHY.
- How do you go about evaluating what training is required and who should provide it? How difficult or easy is this?
    - Have you used any skills or roles frameworks for this before? PROBE AWARENESS/USE OF CHARTERED INSTITUTE FOR INFORMATION SECURITY/IISP, CYBOK, NICE (NATIONAL INITATIVE FOR CYBERSECURITY EDUCATION) AND NIST CYBERSECURITY FRAMEWORK.. How useful are these?
- How do you keep up-to-date with what training products or services are available in the market? How difficult or easy is this? What might make it easier?
- In the last 12 months, what cyber security training has your organisation carried out for:
    - employees in cyber security roles.
    - wider staff.
    - senior managers.
- Which elements of this training were developed internally and which were given by external providers? How satisfied are you with your external training providers?
- How do you evaluate the training that has been given to staff? How effective is it? PROMPT ON INDIRECT OUTCOMES SUCH AS VOLUME OF INCIDENTS OR SUPPORT REQUESTS.
- Where are the gaps in your training? What improvements would you like to see? What changes are you planning or considering?

Role of government

- What role can the government have in supporting training and upskilling in firms like yours and in the industry? What steps can it take? What support can it offer?
- Have you heard of/are you involved in any government-sponsored schemes for cyber skills and training? PROBE ON CYBER FIRST, CYBER DISCOVERY OR THE CYBER SKILLS IMMEDIATE IMPACT FUND. What has your experience of these been? How useful are schemes like this? What can be improved?

Recruitment (c.10 minutes)

Current recruitment

- What would you say are the key issues for your organisation in recruiting people for cyber security roles?
- READ OUT: Have you tried to recruit anyone within the last 3 or so years, i.e. since the beginning of 2015, to fill any cyber skills needs in your organisation? This includes any current vacancies you may have. RECORD ANSWERS.
  - Have any of these vacancies been hard-to-fill? Which ones have been difficult? PROBE ON GENERALIST VS. SPECIALIST ROLES, SENIORITY ETC.
- What were the difficulties? What steps were taken to tackle these? Have you changed your approach? What has worked well? What remains a challenge?
- To what extent has Brexit been an issue in terms of recruiting cyber security roles? What impact do you think it will have in the future?
- What challenges do you think large organisations face more than others around recruitment? PROBE WHETHER PARTICULAR SKILLS NEEDS/PROCEDURES/SYSTEMS UNIQUE TO LARGE ORGANISATIONS.

Recruitment approaches

- What kinds of recruitment methods have you used to fill cyber security roles? PROBE:
  - recruitment agencies (generalist recruitment agency, specialist cyber security recruitment agency)
  - recruitment websites (generalist recruitment websites, e.g. Indeed vs. specialist cyber security recruitment websites, e.g. Cybersecurityjobsite.com)
  - other methods (e.g. social media, direct applications, headhunting, internal recruitment, recruiting from universities/graduate placements, word-of-mouth/industry networks/recommendations).
- What kinds of recruitment approaches work best for you? What makes these effective? How does this vary according to seniority of the role or the types of experience you are looking to recruit?
- How has the way your organisation approaches recruitment changed? And what sort of changes are you likely to see in the future? To what extent is your organisation willing to use new approaches, even if these are untested? PROMPT ON retraining e.g. CSIIF (Cyber Security Immediate Impact Fund) degree and non degree apprenticeships, placement students.
- How do you try to attract candidates? What can and can't you do? PROBE ON SALARY PREMIUMS, BENEFITS, TRAINING OPPORTUNITIES, CAREER PROGRESSION.
- To what extent do you use internal recruitment? How effective has this been?
- Have you recruited less experienced staff and then developed their skills? How successful has this been? What are the challenges and barriers with this approach?

Recruitment criteria

- What do you typically look for in job candidates? How do you weight these different factors? What is more or less important? What makes people stand out? What traits are harder to come by? PROBE ON:
  - EXPERIENCE VS. SENIORITY VS. QUALIFICATIONS
  - TECHNICAL VS. SOFT SKILLS VS. OTHER QUALITIES
  - SPECIALIST VS. GENERALIST SKILLS.
- What do you emphasise in your job descriptions/listings? Does this reflect the kinds of candidates you get?

- How easy is it to know who/what you're looking for? How do you assess candidates and identify what skills they have?
    - Have you used any skills or roles frameworks to guide recruitment? PROBE AWARENESS/USE OF CHARTERED INSTITUTE FOR INFORMATION SECURITY/IISP, CYBOK, NICE (NATIONAL INITATIVE FOR CYBERSECURITY EDUCATION) AND NIST CYBERSECURITY FRAMEWORK. How useful are these?
    - Do you ever use candidate profiling or aptitude testing during recruitment? PROBE ON USE OF APTITUDE TESTING FOR CANDIDATES WITH NO/LITTLE TECHNICAL EXPERIENCE.

Role of government

- What role, if any, does the government have in making it easier for organisations such as yours to recruit new staff for cyber security roles? What steps could they take? What support could they offer?

Diversity (c.5 minutes)

- How diverse would you say your workforce is? What makes you say that?
- How much attention do you pay to diversity? What monitoring do you do? PROBE ON GENDER, ETHNICITY, NEURODIVERSE CONDITIONS.
- What impact does a more diverse workforce have? How do you measure this in your organisation?
- What steps, if any, does your organisation take to encourage diversity when recruiting cyber security staff? PROBE FOR ANY SPECIFIC ACTIONS IN GENERAL AND ON GENDER, ETHNICITY, NEURODIVERSE CONDITIONS IN PARTICULAR.
- How important is this? How much responsibility for this lies with organisations like yours?

Outsourcing (c.10 minutes)

- What aspects of your cyber security are outsourced? PROBE ON SPECIFIC AREAS/TASKS.
- What are the reasons for outsourcing these functions? Why can't you get these skills/roles in-house? How many external providers do you use? How are the provider(s) chosen? How did you/can you assess if your external provider(s) have the right skills?
- How do you monitor/audit the managed services? How often are they audited? How do you know if external providers are doing a good job? What does good look like?
- How big a risk do these external providers pose to your security if things go wrong? What safeguards are in place for this? How do you mitigate against cyber threats being missed?
- Why do you keep other cyber security functions in house? What are the benefits of doing this?
- Have you outsourced cyber security functions in the past and then subsequently brought them in-house? What was behind this change? PROBE ON CHANGES IN INTERNAL CAPABILITIES OR IN EXTERNAL THREATS.
- Which, if any, functions would your organisation not consider outsourcing? Why is that? To what extent has this changed over the past 2-3 years? How might this change in the future?

Wrap-up (2-3 minutes)

- 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? What advice would you give to the government to ensure the cyber skills labour market meets the needs of your organisation?
- GET DETAILS FOR £50 THANK YOU INCENTIVE.
- THANK AND CLOSE.

Cyber Sector organisation

Introduction (2-3 minutes)

- Thank participant for taking part in quantitative survey and explain that DCMS wants to understand in more depth current and future cyber skills gaps, recruitment and training to help inform future government policy.
- Interview should last about 45 minutes.
- Incentives: as a thank you, a £50 incentive will be paid to the participant or a charity of their choice.
- MUST GET PERMISSION TO DIGITALLY RECORD FOR ANALYSIS: Explain recordings will be securely destroyed after the research is complete. If necessary, explain that they will be stored securely and only the research team at Ipsos MORI will have access to these.
- MUST READ OUT AFTER STARTED RECORDING: All responses are confidential and anonymous. DCMS won't know who has taken part and will get an anonymised report pulling out the key findings across all interviews. Participation is voluntary and you can change your mind at any time. Can I confirm you are happy to take part on this basis?
- If you would like to read the privacy policy before we continue, I can give you the link. If you're happy to proceed we'll continue. ADD IF NECESSARY: You can access the privacy policy on our website at: https://ipsos.uk/3993p.

Context (c.3 minutes)

- Tell me a bit about your organisation and your role within it. How long have you been with the organisation?
- What are your day-to-day tasks? How are you involved in skills, training and recruitment decisions? Who else makes decisions around skill, training and recruitment? How many of your cyber security staff are EU nationals?

Skills gaps (c.7 minutes)

Current skills

- To what extent is there a shortage of cyber skills in your organisation? PROBE ON TECHNICAL SKILLS AND SOFT SKILLS, AS WELL AS SENIORITY. Which cyber skillsets or experience is your organisation looking to acquire? What impact is exiting the EU likely to have on your organisation's cyber skills now and in the future?
- What's the impact of these skills gaps or skills shortages on your business? What about on your existing staff?
- What approaches does your organisation take to deal with skills gaps? PROBE ON HIRING, USE OF FREELANCERS/CONSULTANTS.
- To what extent do your cyber teams have to take on multiple roles or adapt their working patterns to address skills shortages? In what ways does your organisation provide support to teams in these cases? PROBE ON HIRING STRATEGY MENTORING, WELFARE INITIATIVES.

Upcoming skills gaps

- Looking to the future, how do you think the needs of the organisation in relation to cyber security might change in the next 5 years? What implications will this have for cyber skills? Are gaps in cyber skills likely to get better or worse? Why is that?
- What potential impact might this have on your organisation? What steps is your organisation taking in relation to this?

Role of government and industry

- What role do cyber security businesses like yours have in addressing cyber skills gaps?
- What role does the government have? What steps should it be taking?

Training (c.10 minutes)

Training requirements

- What are your business's needs in respect of training and upskilling for existing staff? What are the main areas they need training in? PROBE FOR TECHNICAL SKILLS AND SOFT SKILLS. NOTE ANY SPECIFIC TECHNICAL CATEGORIES? What makes these areas so important/a focus?
- IF PARTICIPANT RESPONDED YES AT Q36 OF THE QUANTITATIVE SURVEY: You said in the quantitative survey that in the last 12 months there has been a formal analysis of your organisation's cyber security skills or training needs. What did this involve? Who undertook this analysis and why? PROBE SEPARATELY ON SKILLS AND TRAINING. IF THERE ARE DIFFERENCES, ASK WHY.
- IF PARTICIPANT RESPONDED NO AT Q36 OF THE QUANTITATIVE SURVEY: You said in the quantitative survey that in the last 12 months there has not been a formal analysis of your organisation's cyber security skills or training needs. Why is that? Is this something which is planned for the future? What is this likely to involve? PROBE SEPARATELY ON SKILLS AND TRAINING. IF THERE ARE DIFFERENCES, ASK WHY.
- What training do you offer to your employees? What levels do you offer this at? What role do cyber security-related qualifications or certified training play in training and upskilling your employees?
  - Have you used any skills or roles frameworks for guiding training before? PROBE AWARENESS/USE OF CHARTERED INSTITUTE FOR INFORMATION SECURITY/IISP, CYBOK, NICE (NATIONAL INITATIVE FOR CYBERSECURITY EDUCATION) AND NIST CYBERSECURITY FRAMEWORK.. How useful are these?
- How do you develop and deliver training?
  - Which elements are developed and delivered internally and which are external? What is behind this choice?
  - What are the advantages of internal/external training? What do you think of external cyber security training providers?
  - Have you ever worked in partnership with other organisations, e.g. universities, colleges, to help train staff? Have you considered anything like this? What have been the benefits? What are the challenges?
- How do you evaluate the training given to staff? How effective is it? To what extent is it meeting your organisation's overall training and skills needs?
- Where are the gaps in your training? What improvements would you like to see? What changes are you planning or considering?
- How have your training needs evolved over time? How have you adapted to this? What changes have you made to training over time?

Role of government

- What role can the government have in supporting training and upskilling in firms like yours and in the industry? What steps can it take? What support can it offer?
- Have you heard of/are you involved in any government-sponsored schemes for cyber skills and training? PROBE ON CYBER FIRST, CYBER DISCOVERY OR THE CYBER SKILLS IMMEDIATE IMPACT FUND. What has your experience of these been? How useful are schemes like this? What can be improved?

Recruitment (c.15 minutes)

Current recruitment

- What would you say are the key issues for your organisation in recruiting people for cyber security roles?
- Are there different challenges at different levels? PROBE FOR ENTRY LEVEL, INTERMEDIATE LEVEL, MANAGER, SENIOR MANAGER ETC.
- IF HARD-TO-FILL VACANCIES: You said in the survey that your organisation has found it hard to fill cyber security roles. Could you tell me more about this? How have you dealt with it? Have you changed your approach? What has worked well? What remains a challenge?

- To what extent has Brexit been an issue in terms of recruiting cyber security roles? What impact do you think it will have in the future?

Recruitment approaches

- What kinds of recruitment approaches work best for you? What makes these effective? How does this vary according to seniority of the role or the types of experience you are looking to recruit?
- How do you try to attract candidates? What can and can't you do? PROBE ON SALARY PREMIUMS, BENEFITS, TRAINING OPPORTUNITIES, CAREER PROGRESSION.
- How do the salaries offered for cyber specialists typically differ to those offered to other kinds of technical roles in businesses like yours (e.g. technical IT roles)? What kinds of challenges or pressures does this create? How do you deal with this?
- To what extent do you use internal recruitment? How effective has this been?
- Have you recruited less experienced staff and then developed their skills? How successful has this been? What are the challenges and barriers with this approach?
- How has the way your organisation approaches recruitment changed? And what sort of changes are you likely to see in the future? To what extent is your organisation willing to use new approaches, even if these are untested? PROMPT ON retraining e.g. CSIIF (Cyber Security Immediate Impact Fund) degree and non-degree apprenticeships, placement students.

Recruitment criteria

- What do you typically look for in job candidates? How do you weight these different factors? What is more or less important? What makes people stand out? What traits are harder to come by? PROBE ON:
  - EXPERIENCE VS. SENIORITY VS. QUALIFICATIONS
  - TECHNICAL VS. SOFT SKILLS VS. OTHER QUALITIES
  - SPECIALIST VS. GENERALIST SKILLS.
- What do you emphasise in your job descriptions/listings? Does this reflect the kinds of candidates you get?
- How easy is it to define which cyber skills you are looking for in your recruitment? And how easy is it to assess whether candidates have these skills? How do you assess candidates and identify what skills they have?
  - Have you used any skills or roles frameworks to guide recruitment? PROBE AWARENESS/USE OF CHARTERED INSTITUTE FOR INFORMATION SECURITY/IISP, CYBOK, NICE (NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION) AND NIST CYBERSECURITY FRAMEWORK. How useful are these?
- What kinds of formal qualifications does your organisation look for?
  - What are your minimum educational requirements for job candidates? What made you settle on this?
  - How about specific cyber certifications? PROBE ON CISSP. How about the government's Certified Professional scheme (CCP)? Have you heard of this? What is your opinion of this?
  - What stands out in the market? PROBE FOR SPECIFIC QUALIFICATIONS/CERTIFICATIONS, PROBE ON DIFFERENCE BETWEEN ACADEMIC QUALIFICATIONS (BOTH CYBER AND NON-CYBER RELATED) AND COMMERCIALLY PROVIDED COURSES. What do these qualifications add? How are they different from other cyber-related qualifications?

Role of government

- What role does the government have in making it easier to recruit new staff for cyber security roles? What steps could they take? What support could they offer?

Diversity (c.7 minutes)

- How diverse would you say your workforce is? What makes you say that?
- How much attention do you pay to diversity? What monitoring do you do? PROBE ON GENDER, ETHNICITY, NEURODIVERSE CONDITIONS.

- What impact does a more diverse workforce have? How do you measure this in your organisation?
- What steps, if any, does your organisation take to encourage diversity when recruiting cyber security staff? How important is this? How much responsibility for this lies with organisations like yours?
- You said in the quantitative survey that you have/have not changed or adapted your recruitment processes, or carried out any specific activities to encourage applications from the following groups:
    - Women
    - People from ethnic minority backgrounds
    - People with neurodiverse conditions or learning disorders, such as autism, Asperger's syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD)?
- IF MADE CHANGES IN RESPECT OF ANY GROUP: What steps have been taken? PROBE ON EACH GROUP MENTIONED? What other actions, if any, has your organisation taken to increase diversity? What were the reasons for taking these steps? How effective have these been? How have you evaluated these initiatives? What other plans do you have?
- IF NOT MADE CHANGES IN RESPECT OF ANY GROUP: What actions, if any, has your organisation considered taking to increase diversity? Why is that? PROBE ON EACH GROUP WHERE NO CHANGES MADE. How might that change in the future?
- To what extent does your organisation measure salary disparity for diverse groups? What, if any, disparities have been identified? IF THERE ARE DISPARITIES: And what, if any, action has been or will be taken as a result?
- IF SALARY PREMIUMS PAID: To what extent are salary premiums more likely to be paid to men rather than women? And how about candidates from an ethnic minority? Or with neurodiverse conditions? What action has or may be taken on this? What are your thoughts on using salary premiums to increase diversity?

Wrap-up (2-3 minutes)

- 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? What advice would you give to the government to ensure the cyber skills labour market meets the needs of your business?
- GET DETAILS FOR £50 THANK YOU INCENTIVE.
- THANK AND CLOSE.

Appendix G: inclusion/exclusion criteria for strand 5

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

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

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

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

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

Ipsos MORI’s standards and accreditations

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

ISO 20252

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

ISO 27001

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

ISO 9001

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

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation.

Data Protection Act 2018

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

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

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

About Ipsos MORI Public Affairs

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

Ipsos MORI