Department for Digital, Culture, Media & Sport

Ipsos MORI Social Research Institute

UNIVERSITY OF PORTSMOUTH

Cyber Security Breaches Survey 2019

Technical annex

This technical annex supplements a main statistical release by the Department for Digital, Culture, Media and Sport (DCMS), covering the Cyber Security Breaches Survey 2019. It can be found on the gov.uk website, alongside infographic summaries of the findings, at: https://www.gov.uk/government/collections/cyber-security-breaches-survey.

This annex provides the technical details of the 2019 quantitative survey (fieldwork carried out in winter 2018) and qualitative element (carried out in early 2019), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

The Cyber Security Breaches Survey is a quantitative and qualitative survey of UK businesses and charities. For this latest release, the quantitative survey was carried out in winter 2018 and the qualitative element in early 2019. It helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the Government to shape future policy in this area.

Responsible statistician:

Rishi Vaidya
020 7211 2320

Statistical enquiries:

evidence@culture.gov.uk
@DCMSinsight

General enquiries:

enquiries@culture.gov.uk
0207 211 6200

Media enquiries:

020 7211 2210

Contents

Chapter 1: Overview 1
1.1 Summary of methodology 1
1.2 Strengths and limitations of the survey 1
1.3 Changes from previous waves 2
1.4 Comparability to the earlier Information Security Breaches Surveys 2
Chapter 2: Survey approach technical details 3
2.1 Survey and questionnaire development 3
2.2 Survey microsite 5
2.3 Sampling 5
2.4 Fieldwork 10
2.5 Fieldwork outcomes and response rate 12
2.6 Data processing and weighting 13
2.7 Points of clarification on the data 17
Chapter 3: Qualitative approach technical details 18
3.1 Sampling 18
3.2 Recruitment quotas and screening 18
3.3 Fieldwork 18
3.4 Analysis 20
Appendix A: Pre-interview questions sheet 21
Appendix B: Interviewer glossary 22
Appendix C: Questionnaire 25
Appendix D: Topic guide 61
Appendix E: Further information 68

Chapter 1: Overview

1.1 Summary of methodology

The Cyber Security Breaches Survey 2019 comprised:

- a quantitative random probability telephone survey of 1,566 UK businesses and 514 UK registered charities, carried out from 10 October 2018 to 20 December 2018
- 52 qualitative in-depth interviews, undertaken in January and February 2019 to follow up with organisations that participated in the quantitative survey.

1.2 Strengths and limitations of the survey

While there have been other surveys about cyber security in organisations in recent years, these have often been less applicable to the typical UK business or charity for several methodological reasons, including:

- focusing on larger organisations employing cyber security or IT professionals, at the expense of small organisations (with under 50 staff) that make up the overwhelming majority, and may not employ a professional in this role
- covering several countries alongside the UK, which leads to a small sample size of UK organisations
- using partially representative sampling or online-only data collection methods.

By contrast, the Cyber Security Breaches Survey series is intended to be statistically representative of UK businesses of all sizes and all relevant sectors, and of UK registered charities in all income bands.

The 2019 survey shares the same strengths as previous surveys in the series:

- the use of random-probability sampling to avoid selection bias
- the inclusion of micro and small businesses, and low-income charities, which ensures that the respective findings are not skewed towards larger organisations
- a telephone data collection approach, which aims to also include businesses and charities with less of an online presence (compared to online surveys)
- a comprehensive attempt to obtain accurate spending and cost data from respondents, by using a pre-interview questions sheet and microsite, and giving respondents flexibility in how they can answer (e.g. allowing numeric and banded £ amounts, as well as answers given as percentages of turnover or IT spending)
- a consideration of the cost of cyber security breaches beyond the immediate time-cost (e.g. explicitly asking respondents to consider their direct costs, recovery costs and long-term costs, while giving a description of what might be included within each of these costs).

At the same time, while this survey aims to produce the most representative, accurate and reliable data possible with the resources available, it should be acknowledged that there are inevitable limitations of the data, as with any survey project. The following might be considered the two main limitations:

- Organisations can only tell us about the cyber security breaches or attacks that they have detected. There may be other breaches or attacks affecting organisations, but which are not identified as such by their systems or by staff, such as a virus or other malicious code

that has so far gone unnoticed. Therefore, the survey may have a tendency to systematically underestimate the real level of breaches or attacks.

- When it comes to estimates of spending and costs associated with cyber security, this survey still ultimately depends on self-reported figures from organisations. As previous years' findings suggest, most organisations do not actively monitor the financial cost of cyber security breaches. Moreover, as above, organisations cannot tell us about the cost of any undetected breaches or attacks. Again, this implies that respondents may underestimate the total cost of all breaches or attacks (including undetected ones).

1.3 Changes from previous waves

One of the objectives of the survey is to understand how approaches to cyber security and the cost of breaches are evolving over time. Therefore, the survey methodology is intended to be as comparable as possible to the 2016, 2017 and 2018 surveys.

A small number of questions from the 2016, 2017 and 2018 quantitative surveys were deleted or changed in 2019 to make way for new questions. The changes reflected DCMS priorities, and aimed to improve the survey. Section 2.1 summarises these changes. In the main report, we only make comparisons to 2016, 2017 and 2018 findings where these are valid (i.e. where questions were asked consistently).

1.4 Comparability to the earlier Information Security Breaches Surveys

From 2012 to 2015, the Government commissioned and published annual Information Security Breaches Surveys. While these surveys covered similar topics to the Cyber Security Breaches Survey series, they employed a radically different methodology, with a self-selecting online sample weighted more towards large businesses. Moreover, the question wording and order is different for both sets of surveys. This means that comparisons between surveys from both series are not possible.

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

Ipsos MORI developed the questionnaire and all other survey instruments (e.g. the interview script and respondent microsite), which DCMS then approved. Development for this year's survey took place over three stages from July to September 2018:

- stakeholder conversations with the Association of British Insurers (ABI), the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB) and the Institute of Chartered Accountants in England and Wales (ICAEW).
- cognitive testing interviews with four businesses and four charities
- a pilot survey, consisting of 19 interviews with businesses and 21 with charities.

Stakeholder conversations

The stakeholder conversations were intended to:

- clarify the key cyber security issues facing organisations, including any new issues arising since the 2018 survey
- review the 2018 questionnaire, survey instruments and findings, to assess gaps in knowledge and new question areas to be included in 2019.

Before this stage, the DCMS team had already liaised with various Government stakeholders about the survey. Based on these discussions and their own internal thinking, DCMS decided to keep as much of the survey as consistent as possible with previous years, with only a small number of specific questionnaire changes and improvements made for this year.

Given that DCMS anticipated very few changes to the questionnaire this year, the more intensive stakeholder workshops and in-depth interviews carried out in previous years were not needed. Instead, Ipsos MORI gathered feedback from representatives of the ABI, CBI, the FSB, ICAEW and our research partners, the Institute of Criminal Justice Studies (ICJS), through emails and telephone conversations.

Following this stage, we amended the 2018 questionnaire with provisional new questions for testing, guided by DCMS. The changes were minor and were as follows:

- We added new questions to explore:
  - when cyber security policies were last reviewed
  - two-factor authentication (a late addition, which we were not able to cognitively test and has not been included in the main report – see Section 3.4)
  - awareness of the implications of GDPR.
- We amended the wording of RULES around personal data encryption to make clearer what was being asked.
- To allow space for new questions, we deleted four questions from 2018. This was either because they had been of limited use in previous years, or because DCMS felt they covered the same ground as other questions in the survey.
  - CHARITYO was a question splitting the charity sample into subgroups by charitable area. This information was not used in reporting last year due to low subgroup sample sizes, so was removed on that basis.
  - CORE was similar to ONLINE (both covered organisations' online exposure).
  - DOC overlapped with MANAGE and IDENT (covering documentation of cyber risks).
  - CONTING was similar to INCID (covering incident response plans).

- We amended the survey and microsite introductions, and recontact question wording. These were made shorter, to better encourage participation. We also added the necessary text and an upfront screener question to gain explicit consent from respondents, in line with General Data Protection Regulation (GDPR) requirements.

Cognitive testing

The Ipsos MORI research team carried out eight cognitive testing interviews to test comprehension of new questions for 2019, and also to review the survey introduction and the new encouragements for taking part (the offer of a Government guidance help card and an electronic copy of the survey findings).

We recruited all participants by telephone. We purchased the business sample from the Dun & Bradstreet business directory, and took a random selection of charities from the charity regulator databases in each UK country. We applied recruitment quotas and offered £50 incentive[1] to ensure different-sized organisations from a range of sectors or charitable areas took part.

After this stage, the questionnaire was tweaked. The changes were very minor.

- We updated the answer scale for REVIEW.
- We chose between alternative versions of the new GDPR-related questions (the ones relating to fines and reporting of breaches to the Information Commissioner's Office). We removed the ones that had a definitely true–definitely false scale (where the correct answers were easy for participants to guess).

Pilot survey

The pilot survey was used to:

- test the questionnaire CATI (computer-assisted telephone interviewing) script
- time the questionnaire
- test the usefulness of the written interviewer instructions and glossary
- explore likely responses to questions with an "other WRITE IN" option (where respondents can give an answer that is not part of the existing pre-coded list)
- test the quality and eligibility of the sample (by calculating the proportion of the dialled sample that ended up containing usable leads).

Ipsos MORI interviewers carried out all the pilot fieldwork between 24 and 28 September 2018. Again, we applied quotas to ensure the pilot covered different-sized businesses from a range of sectors, and charities with difference incomes and from different countries. We carried out with 19 interviews with businesses and 21 with charities (40 in total).

The pilot sample came from the same sample frames used for the main stage survey for businesses and charities (see next section). In total, we randomly selected 320 business leads and 290 charity leads.

Not all these leads were used to complete the 40 pilot interviews. In the end, 117 untouched business leads and 4 charity leads from the pilot were released again for use in the main stage survey.

The questionnaire length for the pilot was 22 minutes, which was on target for the main stage. Following feedback from the pilot survey, we made some minor changes to the questionnaire:

- further shortening the introduction

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

- grouping the pre-coded responses into categories at NOINSURE for easier response allocation
- adding “Charity Commission” as an answer code at REPORTB.

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

2.2 Survey microsite

As in previous years, a publicly accessible microsite[2] (still active as of April 2019) was again used to:

- provide reassurance that the survey was legitimate
- promote the survey endorsements
- provide more information before respondents agreed to take part
- allow respondents to prepare spending and cost data for the survey before taking part
- allow respondents to give more accurate spending and cost data *during the interview*, by laying out these questions on the screen, including examples of what came under each type of cost (e.g. “staff not being able to work” being part of the direct costs of a breach).

The survey questionnaire included a specific question where interviewers asked respondents if they would like to use the microsite to make it easier for them to answer certain questions. At the relevant questions, respondents who said yes were then referred to the appropriate page or section of the microsite, while others answered the questionnaire in the usual way (with the interviewer reading out the whole question).

2.3 Sampling

Business population and sample frame

The target population of businesses matched those included in the 2018, 2017 and 2016 surveys:

- private companies or non-profit organisations[3] with more than one person on the payroll
- universities and independent schools or colleges.[4]

The survey is designed 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 IT devices and will therefore deal with cyber security centrally.

The sample frame for businesses was the Government’s Inter-Departmental Business Register (IDBR), which covers businesses in all sectors across the UK at the enterprise level. This is one of the main sample frames for Government surveys of businesses and for compiling official statistics.

Review of alternative sampling frames

At the development stage this year, Ipsos MORI carried out a review of sampling approaches to ensure the sampling frame being used for the survey remained fit for purpose. We reviewed

[2] See https://csbs.ipsos-mori.com/ for the Cyber Security Breaches Survey microsite (active as of publication of this statistical release).

[3] These are organisations that work for a social purpose, but are not registered as charities, so not regulated by their respective Charity Commission.

[4] These are typically under SIC 2007 category P. Where these organisations identified themselves to be charities, they were moved to the charity sample.

several alternative potential sample frames, including the following commercial business databases:

- Dun & Bradstreet
- Experian
- Market Location.

These commercial sample frames have some advantages over the IDBR. For example:

- With the IDBR, businesses selected in the micro category (with 1 to 9 staff) have sometimes turned out to be sole traders (with 0 staff), who are not eligible for this survey. This accounted for 1 per cent of the sample in 2019 and 2 per cent in 2018. Commercial sample frames typically produce samples with a higher eligibility rate, because they tend to have fewer businesses misclassified as sole traders.
- A high majority of records come with a switchboard number for the business, as well as a key decision-maker contact name. This contrasts with the low telephone coverage for the IDBR (13% of the selected IDBR sample had telephone numbers this year). The

However, there were downsides to the commercial sampling frames too. For example:

- The commercial sample frames have far fewer records overall than the IDBR, ranging from c.700,000 to c.1 million, compared to c.2 million for the IDBR. A survey sample achieved from any of these sample frames can be weighted on observable variables, such as size and sector, to match the overall business population profile. However, we cannot weight to correct for non-observable differences between the types of businesses in each frame. Therefore, the representativeness of a sample achieved through a commercial frame may be called into question when compared to surveys using the IDBR.
- The IDBR is compiled in a transparent and very consistent way each year. The way commercial frames are compiled is less transparent and, hence, potentially subject to unknown changes each year. With a commercial frame, therefore, users may not have the same level of confidence in the survey tracking legitimate changes in attitudes or behaviours over time. Any unusual changes in results might simply reflect changes in the types of businesses represented in the sample frame for that particular year.

Consequently, following this review, we agreed with DCMS that it was best to continue to use the IDBR in this year's survey.

Exclusions from the IDBR sample

With the exception of universities, public sector organisations are typically subject to Government-set minimum standards on cyber security. Moreover, the focus of the survey was to provide evidence on businesses' engagement, to inform future policy for this audience. Public sector organisations (Standard Industrial Classification, or SIC, 2007 category O) were therefore considered outside of the scope of the survey and excluded from the sample selection.

As in all previous years, organisations in the agriculture, forestry and fishing sectors (SIC 2007 category A) were also excluded. There are practical considerations that make it challenging to interview organisations in this relatively small sector, as this requires additional authorisation from the Department for Environment, Food and Rural Affairs if sampling from the IDBR. We also judged cyber security to be a less relevant topic for these organisations, given their relative lack of e-commerce.

Charity population and sample frames (including limitations)

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 Office of 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/.

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 yet have a comprehensive list of established charities. It is in the process of registering charities and building one. Alternative sample frames for Northern Ireland, such as the Experian and Dun & Bradstreet business directories (which also include charities) were considered, and ruled out, because they did not contain essential information on charity income for sampling, and cannot guarantee up-to-date charity information.

Therefore, while the Charity Commission in Northern Ireland database was the best sample frame for this survey, it cannot be considered as a truly random sample of Northern Ireland charities at present. This situation appears, however, to have slightly improved since the 2018 survey (the first to include charities); in 2019, there were 6,078 registered charities on the Northern Ireland database, compared to 5,811 in 2018.

Sample selection

In total, 77,432 businesses were selected from the IDBR for the 2019 survey. This is much higher than the 53,783 businesses selected for the 2018 survey, and the 27,948 selected in the 2017 survey. We chose the higher number to ensure there was enough reserve sample to meet the size-by-sector survey targets, based on the sample quality of the two previous waves. In the 2018 survey, we had used up all reserve sample in the largest size band. There had also been a successive decline in sample quality (in terms of telephone coverage and usable leads) in both 2017 (vs. 2016) and 2018 (vs. 2017). Ultimately, the 2019 sample quality turned out to be equivalent to the 2018 sample (with a very slightly higher proportion of usable leads), leaving us with sufficient usable leads because of the higher selection count.

The business sample was proportionately stratified by region, and disproportionately stratified by size and sector. An entirely proportionately stratified sample would not allow sufficient subgroup analysis by size and sector. For example, it would effectively exclude all medium and large businesses from the selected sample, as they make up a very small proportion of all UK businesses. Therefore, we set disproportionate sample targets for micro (1 to 9 staff), small (10 to 49 staff), medium (50 to 249 staff) and large (250 or more staff) businesses. We also boosted specific sectors, to ensure we could report findings for the same sector subgroups that were used in the 2018 report. The boosted sectors included:

- education
- entertainment; service or membership organisations
- health, social work or social care
- information and communications
- transport and storage.

Post-survey weighting corrected for the disproportionate stratification (see section 2.6).

Table 2.1 breaks down the selected business sample by size and sector.

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

SIC 2007 letter[5]	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)	1,533	356	628	2,517
F	Construction	8,137	118	113	8,368
G	Retail or wholesale (including vehicle sales and repairs)	5,974	271	734	6,979
H	Transport or storage	6,110	186	344	6,640
I	Food or hospitality	4,315	233	169	4,717
J	Information or communications	11,411	180	387	11,978
K	Finance or insurance	1,100	249	383	1,732
L, N	Administration or real estate	8,195	218	447	8,860
M	Professional, scientific or technical	12,697	191	385	13,273
P	Education	4,300	137	118	4,555
Q	Health, social care or social work	3,647	199	180	4,026
R, S	Entertainment, service or membership organisations	3,529	97	161	3,787
	Total	**70,948**	**2,435**	**4,049**	**77,432**

The charity sample was proportionately stratified by country and disproportionately stratified by income band. This used the same reasoning as for businesses – without this disproportionate stratification, analysis by income band would not be possible as hardly any high-income charities would be in the selected sample. As the entirety of the three charity regulator databases were used for sample selection, there was no restriction in the amount of charity sample that could be used, so no equivalent to Table 2.1 is shown for charities.

Sample telephone tracing and cleaning

Not all the original sample was usable. In total, 67,434 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 (matching the database to both the UK Changes business and residential number databases) to fill in the gaps where possible. No telephone tracing was required for charities from England and Wales, and Northern Ireland.

The selected sample was also cleaned to remove any duplicate telephone numbers, as well as the small number of state-funded schools or colleges that were listed as being in the education sector (SIC 2007 category P) but were actually public-sector organisations.

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

At the same time as this survey, Ipsos MORI was also carrying out two other business surveys with potentially overlapping samples. These were the Commercial Victimisation Survey 2019 for the Home Office; and another survey on attitudes to cyber security commissioned by the National Cyber Security Centre. We therefore removed overlapping sample leads from this survey to avoid contacting the same organisations for multiple surveys.

Following telephone tracing and cleaning, the usable business sample amounted to 15,358 leads (including the leads taken forward from the pilot). For the Scotland charities sample, 3,546 leads had telephone numbers after matching.

Table 2.2 breaks the usable business leads down by size and sector. As this shows, there was typically much greater telephone coverage in the medium and large businesses in the sample frame than among micro and small businesses. This has been a common pattern across years. In part, it reflects the greater stability in the medium and large business population, where firms tend to be older and are less likely to have recently updated their telephone numbers.

Table 2.2: Post-cleaning available main stage sample by size and sector

SIC 2007 letter	Sector description	Micro or small (1–49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
B, C, D, E	Utilities or production (including manufacturing)	465	325	543	1,333
		30%	91%	86%	53%
F	Construction	1,091	103	99	1,293
		13%	87%	88%	15%
G	Retail or wholesale (including vehicle sales and repairs)	1,663	230	347	2,240
		28%	85%	47%	32%
H	Transport or storage	612	169	274	1,055
		10%	91%	80%	16%
I	Food or hospitality	1,038	176	99	1,313
		24%	76%	59%	28%
J	Information or communications	686	142	308	1,136
		6%	79%	80%	9%
K	Finance or insurance	708	216	344	1,268
		64%	87%	90%	73%
L, N	Administration or real estate	897	174	375	1,446
		11%	80%	84%	16%
M	Professional, scientific or technical	1,243	170	297	1,710
		10%	89%	77%	13%
P	Education	537	117	102	756
		12%	85%	86%	17%
Q	Health, social care or social work	524	182	157	863

SIC 2007 letter	Sector description	Micro or small (1–49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
		14%	91%	87%	21%
R, S	Entertainment, service or membership organisations	724	78	143	945
		21%	80%	89%	25%
	Total	**10,188**	**2,082**	**3,088**	**15,358**
		14%	**86%**	**76%**	**20%**

The usable leads for the main stage survey were randomly allocated into separate batches for businesses and charities. The first business batch included 5,451 leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band from the 2018 survey. In other words, more sample was selected in sectors and size bands where there was a higher target, or where response rates were relatively low last year. The first charity batch had 912 leads matching the disproportionate targets by income band.

Subsequent batches were drawn up and released as and when live sample was exhausted. Not all available leads were released in the main stage (see Tables 2.3 and 2.4).

2.4 Fieldwork

Ipsos MORI carried out all main stage fieldwork was from 10 October 2018 to 20 December 2018 using a Computer-Assisted Telephone Interviewing (CATI) script. This was a similar overall fieldwork period as for the 2018 survey.

In total, we completed 1,566 interviews with businesses, and 514 with charities. The average interview length was 22 minutes for businesses and 23 minutes for charities.

Fieldwork preparation

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

- written instructions about all aspects of the survey
- a copy of the questionnaire and other survey instruments
- a glossary of unfamiliar terms (included in Appendix B).

Screening of respondents

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

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

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 it was established that the organisation was eligible, and that this was the head office, interviewers were told to identify the senior member of staff who has the most knowledge or responsibility when it comes to cyber security.

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

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

Random-probability approach and maximising participation

We adopted random-probability sampling to minimise selection bias. The overall aim with this approach is to have a known outcome for every piece of sample loaded. For this survey, an approach comparable to other robust business surveys was used around this:

- Each organisation loaded in the main survey sample was called either a minimum of 7 times, or until an interview was achieved, a refusal given, or information obtained to make a judgment on the eligibility of that contact. Overwhelmingly (in 95% of cases), leads were called 10 times or more before being marked as reaching the maximum number of tries. For example, this outcome was used 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. Evening and weekend interviews were also offered if the respondent preferred these times.

We took several steps to maximise participation in the survey and reduce non-response bias:

- Interviewers could send the reassurance email to prospective respondents if the respondent requested this.
- The survey had its own web page on the Government's GOV.UK and the Ipsos MORI websites, to let businesses know that the contact from Ipsos MORI was genuine. The web pages included appropriate Privacy Notices on processing of personal data, and the data rights of participants, following the introduction of GDPR in May 2018.
- The survey was endorsed by the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), the Institute of Chartered Accountants in England and Wales (ICAEW), the Association of British Insurers (ABI), TechUK, the Charity Commission for England and Wales and the Charity Commission for Northern Ireland meaning that they allowed their identity and logos to be used in the survey introduction and on the microsite, to encourage businesses to take part.
- As an extra encouragement, used for the first time in 2019, we offered to send respondents an electronic copy of the survey findings, and a help card listing the range of Government guidance on cyber security, following their interview.

Fieldwork monitoring

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

2.5 Fieldwork outcomes and response rate

We monitored fieldwork outcomes and response rates throughout fieldwork, and interviewers were given regular guidance on how to avoid common reasons for refusal. Table 2.3 shows the final outcomes and the adjusted response rate calculations for businesses and charities.[6]

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

Table 2.3: Fieldwork outcomes and response rate calculations for businesses and charities

Outcome	Total for businesses	Total for charities
Total sample loaded	10,229	1,486
Completed interviews	1,566	514
Incomplete interviews	50	13
Ineligible leads – established during screener[7]	131	3
Ineligible leads – established pre-screener	205	54
Refusals[8]	1,855	132
Unusable leads with working numbers[9]	694	628
Unusable numbers[10]	1,181	94
Working numbers with unknown eligibility[11]	4,547	548
Expected eligibility of screened respondents[12]	93%	99%

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

[7] 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.

[8] This excludes “soft” refusals. This is where the respondent was initially hesitant about taking part, so our interviewers backed away and avoided a definitive refusal.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

Outcome	Total for businesses	Total for charities
Expected eligibility of working numbers[13]	74%	78%
Unadjusted response rate	15%	35%
Adjusted response rate	23%	47%
Cooperation rate[14]	47%	80%

The adjusted response rate for businesses in the 2019 survey was moderately lower than for 2018 (25%). The reasons for this are unclear, but the low response rate overall across businesses reflects the challenge of surveying organisations on this topic. Many organisations did not want to take part and reveal what they considered as commercially confidential information, while many were also concerned about the survey not being bona fide. It may be the case that, as the saliency of cyber attacks increases, organisations are becoming slightly less willing to engage in conversations about their approaches to cyber security.

Several steps have been taken each year to reduce these barriers to taking part, including reassurances around confidentiality and setting up the survey microsite.

The adjusted response rate for charities is considerably higher than in the 2018 survey (when it was 36%). This is the second year that the survey has been carried out with charities. The improvement may, in part, reflect that the interviewer team were more experienced with this research audience than in 2018.

2.6 Data processing and weighting

Editing and data validation

There were a number of logic checks in the CATI script, which checked the consistency and likely accuracy of answers estimating spending, turnover, costs, number of cyber security breaches and time spent dealing with breaches. If respondents gave unusually high or low answers at these questions relative to the size of their organisation, the interviewer would read out the response they had just recorded and double-check this is what the respondent meant to say. This meant that, typically, no post-fieldwork editing has been required to remove outliers.

This year, we did remove one outlier value for the turnover question after fieldwork. This value had triggered a logic check in the CATI script and the interviewer had revalidated the answer with the respondent. However, based on their other answers and the nature of their business, the value was not credible. This one value was considerably skewing the mean score estimates of investment in cyber security, so we have manually adjusted it in the final dataset to a “don’t know” response.

Coding

The verbatim responses to unprompted questions could be coded as “other” by interviewers when they did not appear to fit into the predefined code frame. These “other” responses were coded manually by Ipsos MORI’s coding team, and where possible, were assigned to codes in

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

[14] The cooperation rate has been calculated as: (completed interviews + incomplete interviews) / (completed interviews + incomplete interviews + refusals). This is the proportion who took part in the survey, among those who were reached and screened.

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 Ipsos MORI research team verified the accuracy of the coding, by checking and approving each new code proposed.

We did not undertake SIC coding. Instead the SIC 2007 codes that were already in the IDBR sample were used to assign businesses to a sector for weighting and analysis purposes. The pilot survey in 2016 had overwhelmingly found the SIC 2007 codes in the sample to be accurate, so this practice was carried forward to subsequent surveys.

Weighting

We applied rim weighting (random iterative method weighting) to account where possible for non-response bias, and also to account for disproportionate sampling (by size and sector for businesses, and by income band for charities). The intention was to make the weighted data representative of the actual UK business and UK registered charities populations. Rim weighting is a standard weighting approach undertaken in business surveys of this nature. In cases where the weighting variables are strongly correlated with each other, it is potentially less effective than other methods, such as cell weighting. However, this is not the case for this survey.

In line with the weighting approaches from the 2018, 2017 and 2016 surveys, non-interlocking rim weighting by size and sector was undertaken for businesses. We did not weight by region, primarily because region is not considered to be an important determining factor for attitudes and behaviours around cyber security. Moreover, the final weighted data are already closely aligned with the business population region profile.

Non-interlocking rim weighting by income band and country was undertaken for charities.

For both businesses and charities, interlocking weighting was also possible, but was ruled out as it would have potentially resulted in very large weights. This would have reduced the statistical power of the survey results, without making any considerable difference to the weighted percentage scores at each question.

Table 2.4 and Table 2.5 shows the unweighted and weighted profiles of the final data.

Table 2.4: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Micro or small (1–49 staff)	69%	97%
Medium (50–249 staff)	18%	3%
Large (250+ staff)	13%	1%
Sector		
Administration or real estate	11%	13%
Construction	8%	13%
Education	6%	1%
Entertainment, service or membership organisations	6%	7%
Finance or insurance	7%	2%

	Unweighted %	Weighted %
Food or hospitality	8%	10%
Health, social care or social work	5%	5%
Information or communications	7%	6%
Professional, scientific or technical	11%	15%
Retail or wholesale (including vehicle sales or repairs	14%	18%
Transport or storage	8%	4%
Utilities or production (including manufacturing)	9%	7%

Table 2.5: Unweighted and weighted sample profiles for charity interviews

	Unweighted %	Weighted %
Income band		
£0 to under £10,000	16%	38%
£10,000 to under £100,000	14%	32%
£100,000 to under £500,000	27%	12%
£500,000 to under £5 million	20%	5%
£5 million or more	20%	1%
Unknown income	3%	11%
Country		
England and Wales	91%	84%
Northern Ireland	2%	4%
Scotland	7%	12%

Reporting of two-factor authentication question

The RULES question this year had a new code added at a late stage, after the cognitive testing and pilot survey. It asked organisations if they had “two-factor authentication to access restricted files, or log into your own websites or apps”.

Based on the very high proportion of businesses (48%) and charities (34%) saying they had this form of technical control in their organisation, we believe this question has been misinterpreted – without organisations fully understanding what two-factor authentication is and what it is not. We gathered retrospective cognitive testing evidence on this in the follow-up qualitative interviews, and found that many organisations had not answered the question with a full understanding.

We have therefore decided not to report on this question in the SPSS dataset (covered later in this section) or in the main report, because the results risk being misleading in this instance.

Derived variables

At certain questions in the survey, respondents were asked to give either an approximate numeric response or, if they did not know, then a banded response (e.g. for spending on cyber

security). The vast majority (typically around eight in ten) of those who gave a response (excluding refusals) gave numeric responses. It has been agreed with DCMS from the outset of the survey that for those who gave banded responses, a numeric response would be imputed. This ensured that no survey data went unused and also allowed for larger sample sizes for these questions.

To impute numeric responses, syntax was applied to the SPSS dataset which:

- calculated the mean amount within a banded range for respondents who had given numeric responses (e.g. a £200 mean amount for everyone giving an answer less than £500)
- applied this mean amount as the imputed value for all respondents who gave the equivalent banded response (i.e. £200 would be the imputed mean amount for everyone not giving a numeric response but saying “less than £500” as a banded response).

Often in these cases, a common alternative approach is to take the mid-point of each banded response and use that as the imputed value (i.e. £250 for everyone saying “less than £500”). It was decided against doing this for this survey given that the mean responses within a banded range tended to cluster towards the bottom of the band. This suggested that imputing values based on mid-points would slightly overestimate the true values across respondents.

Associated datasets

A de-identified SPSS dataset will also be published on the UK Data Archive to enable further analysis. Wherever possible, the variables are consistent with those in the 2018 and 2017 survey datasets.

No numeric £ variables will be included in this dataset. This was agreed with DCMS to prevent any possibility of individual organisations being identified. Instead, all variables related to spending and cost figures will be banded, including the imputed values (laid out in the previous section). These banded variables include:

- one variable (investn_bands) with derived values (banded rather than numeric) for the £ amount invested in cyber security, including imputed banded values when respondents answered as a percentage of turnover or of IT spending
- derived variables related to the cost of cyber security breaches or attacks
    - the estimated cost of all breaches experienced in the last 12 months (cost_bands)
    - the estimated direct results cost of the most disruptive breach or attack (damagedirx_bands)
    - the estimated recovery cost of the most disruptive breach or attack (damagerecx_bands)
    - the estimated long-term cost of the most disruptive breach or attack (damagelonx_bands)
    - the sum-total of estimated costs of the most disruptive breach or attack, merging responses across damagedirx, damagerecx and damagelonx (damage_bands).

In addition, the following merged or derived variables will be included:

- number of breaches experienced in the last 12 months (numb)
- how long it took to deal with the most disruptive breach or attack (deal)
- merged region (region_comb), which includes collapsed region groupings to ensure that no individual respondent can be identified

- a merged sector variable (sector_comb2), which matches the sector groupings used in the 2019 and 2018 main reports
- derived variables showing which steps from the Government's 10 Steps guidance have been implemented in some form (as per the definition in the main report, the variables are Step1, Step2 etc)
- derived variables showing if a business has taken any of the 10 Steps (Any10Steps) and how many of the 10 Steps they have taken (Sum10Steps).

Rounding differences between the SPSS dataset and published data

If running analysis on weighted data in SPSS, users must be aware that the default setting of the SPSS crosstabs command does not handle non-integer weighting in the same way as typical survey data tables.[15] Users may therefore see very minor differences in results (no more than one percentage point, and on rare occasions) between the SPSS dataset and the percentages in the main release and infographics, which consistently use the survey data tables.

2.7 Points of clarification on the data

Sector grouping

In the SPSS datasets for previous years of the survey, an alternative sector variable (sector_comb1) was included. This variable grouped some sectors together in a different way, and was less granular than the updated sector variable (sector_comb2).

- "education" and "health, social care or social work" were merged together, rather than being analysed separately
- "information or communications" and "utilities" were merged together, whereas now "utilities" and "manufacturing" are merged together.

The previous grouping reflected how we used to report on sector differences before the 2018 survey. As this legacy variable has not been used in the report for the last two years, we have stopped including it in the SPSS dataset, in favour of the updated sector variable.

Questions on outsourcing cyber security

The SPSS dataset has two variables covering use of external cyber security providers:

- OUTSOURCE (Q9)
- MANAGE2 (Q29).

Both questions collect the same data – about the proportion of organisations that outsource cyber security – but are asked at two different points in the questionnaire, in slightly different ways. As expected, the answers for each question are very similar, but a handful of respondents answer in a different way for each question. In the main report, we only quote the figures from OUTSOURCE (Q9). It offers a more granular snapshot than MANAGE2, showing both those that currently outsource, and those that intend to do so.

The MANAGE2 question was kept in the questionnaire. This was mainly to keep the routing into the subsequent NOPOL (Q29B) question unchanged since the 2016 survey.

[15] The default SPSS setting is to round cell counts and then calculate percentages based on integers.

Chapter 3: Qualitative approach technical details

3.1 Sampling

We took the sample for the 52 in-depth interviews from the quantitative survey. We asked respondents during the quantitative survey whether they would be willing to be recontacted specifically to take part in a further 45-minute interview on the same topic as the survey. In total, 741 businesses (47%) and 276 charities (54%) agreed to be recontacted.

Ultimately, we carried out 32 interviews with businesses and 20 with charities.

3.2 Recruitment quotas and screening

We carried out recruitment for the qualitative element by telephone, using a specialist business recruiter. We offered a cheque or charity donation made on behalf of participants to encourage participation. This was initially set at £50, and increased to £60 in the latter half of fieldwork.

We used recruitment quotas to ensure that interviews included a mix of different sizes, sectors and regions for businesses, and different charitable areas, income bands and countries for charities. We also had further quotas based on the responses in the quantitative survey, reflecting the topics to be discussed in the interviews. These ensured we spoke to a range of organisations:

- where directors or trustees see cyber security as a fairly or very high priority
- that have made changes to cyber security as a result of GDPR
- that required suppliers to meet cyber security standards
- that have used Government sources of information and guidance
- with cyber insurance
- that outsource their cyber security
- that have experienced a financially costly cyber security breach in the last 12 months.

These were all administered as soft rather than hard quotas. This meant that the recruiter aimed to recruit a minimum number of participants in each group, and could exceed these minimums, rather than having to reach a fixed number of each type of respondent.

We also briefed the recruiter to carry out a further qualitative screening process of participants, to check that they felt capable of discussing at least some of the broad topic areas covered in the topic guide (laid out in the following section). The recruiter probed participants' job titles, job roles, and gave them some further information about the topic areas over email. The intention was to screen out organisations that might have been willing to take part but would have had little to say on these topics. After early feedback from this approach, we also decided to exclude very low-income charities (with under £10,000) from the sample entirely.

3.3 Fieldwork

The Ipsos MORI research team carried out all fieldwork from in January and February 2019. We conducted 44 interviews by telephone and 8 face-to-face, based on what the participant preferred. Interviews lasted around 45 minutes on average.

DCMS originally laid out their topics of interest for 2019. Ipsos MORI then drafted the interview topic guide around these topics, which was reviewed and approved by DCMS. The qualitative topic guide has changed each year much more substantially than the quantitative questionnaire, in order to respond to the new findings that emerge from each year's quantitative survey. The intention is for the qualitative research to explore new topics that were not necessarily as big or salient in previous years (such as GDPR), as well as to look more in depth at the answers that

organisations gave in this year's survey. This year, the guide covered the following broad question areas:

- What drives the prioritisation of cyber security within organisations? What does treating it as a high priority look like in practice? How has this prioritisation changed in the past year?
- How has GDPR impacted approaches to cyber security? Is any impact of GDPR expected to last in the long term?
- How do organisations consider and manage cyber security risk from suppliers?
- What are organisations' main sources of information and guidance on cyber security? What type of information or guidance is considered most useful? What do they think of Government information and guidance in particular?
- What drives organisations to take up cyber security insurance? What impact has cyber insurance had on behaviour?
- How does outsourcing cyber security impact on attitudes towards risk?
- When estimating the cost of cyber security breaches, what factors are taken into account?

There was not enough time in each interview to ask about all these topics, so we used a modular topic guide design, where the researcher doing the interview would know beforehand to only focus on a selection of these areas. Across the course of fieldwork, the core research team reviewed the notes from each interview and gave the fieldwork team guidance on which topics needed further coverage in the remaining interviews. This ensured we asked about each of these areas in a wide range of interviews, with at least 18 interviews covering each topic.

A full reproduction of the topic guide is available in Appendix D.

Tables 3.1 and 3.2 shows a profile of the 32 interviewed businesses by size and sector.

Table 3.1: Sector profile of businesses in follow-up qualitative stage

SIC 2007 letter	Sector description	Total
B, C, D, E	Utilities or production (including manufacturing)	4
F	Construction	2
G	Retail or wholesale (including vehicle sales and repairs)	6
H	Transport or storage	2
I	Food or hospitality	0
J	Information or communications	3
K	Finance or insurance	5
L, N	Administration or real estate	1
M	Professional, scientific or technical	4
P	Education (excluding further or higher education institutions)	0
Q	Health, social care or social work	1
R, S	Entertainment, service or membership organisations	4
	Total	**32**

Table 3.2: Size profile of businesses (by number of staff) in follow-up qualitative stage

Size band	Total
Micro or small (1–49 staff)	11
Medium (49–249 staff)	10
Large (250+ staff)	11

Table 3.3 shows a profile of the 20 interviewed charities by income band.

Table 3.3: Size profile of charities (by income band) in follow-up qualitative stage

Income band	Total
£10,000 to under £100,000	1
£100,000 to under £500,000	5
£500,000 to under £5 million	4
£5 million or more	10

Cyber insurance in the news during fieldwork

Just before the start of qualitative fieldwork in January 2019, there was a news story on cyber insurance that appeared in a small number of UK newspapers, news websites and technology websites. It discussed the decision by Zurich American Insurance Company to not pay out on a cyber insurance claim by US company Mondelēz, after they were affected by the substantive NotPetya ransomware attack.[16] Overall, we do not believe this had a major impact on the qualitative findings, although a small number of participants did mention hearing about this story when discussing the benefits and drawbacks of cyber insurance in the interviews.

3.4 Analysis

Throughout fieldwork, the core research team discussed interim findings and outlined areas to focus on in subsequent interviews. Specifically, we held two face-to-face analysis meetings with the entire fieldwork team – one halfway through fieldwork and one towards the end of fieldwork. In these sessions, researchers discussed the findings from individual interviews and we drew out emerging key themes, recurring findings and other patterns across the interviews. DCMS attended both these sessions and helped identify what they saw as the most important findings, as well as areas worth exploring further in the remaining interviews.

We also recorded all interviews and summarised them in an Excel notes template, which categorised findings by topic area and the research questions within that topic area. The research team reviewed these notes, and also listened back to recordings, to identify the examples and verbatim quotes to include in the main report.

[16] See, for example, this story in the Financial Times on 9 January 2019: https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e.

Appendix A: Pre-interview questions sheet

Thanks for agreeing to take part in this important Government survey. Below are some of the questions the Ipsos MORI interviewer will ask over the phone. Other participants have told us it is helpful to see these questions in advance, so they can **talk to relevant colleagues and get the answers ready before the call**.

- This helps make the interview shorter and easier for you.
- These answers are totally confidential and anonymous for all individuals and organisations.
- We will get your answers when we call you. You do not need to send them to us.

	Your answers
In your last financial year just gone, approximately how much, if anything, did you invest in cyber security? ..... *This is spending on any activities or projects to prevent or identify cyber security breaches or attacks (software, hardware, staff salaries, outsourcing, training costs etc). Please <u>exclude</u> any spending on repair or recovery from breaches or attacks.* *To make it easiest for you, you only need to answer in <u>one</u> of the following ways:* • *As a number in £s* • *Or as a % of turnover or income* • *Or as a % of total IT expenditure*	**£** **%** **of turnover or income** **%** **of total IT expenditure** **in last <u>financial year</u>**
When it comes to cyber security insurance, which of the following best describes your situation? ..... *A. We have a specific cyber security insurance policy* *B. We do not currently have a specific cyber security insurance policy, but have previously considered it* *C. We do not currently have a specific cyber security insurance policy and have not previously considered it*	A / B / C
Have you ever made any insurance claims for cyber security breaches under this insurance before?	Yes **/** No
In the last 12 months, approximately how much, if anything, do you think cyber security breaches or attacks have cost your organisation <u>in total</u> financially? ..... *This might include any of the following costs:* • *Staff stopped from carrying out day-to-day work* • *Loss of revenue or share value* • *Extra staff time to deal with the breach or attack, or to inform stakeholders* • *Any other repair or recovery costs* • *Lost or stolen assets* • *Fines from regulators or authorities, or associated legal costs* • *Reputational damage* • *Prevented provision of goods or services to customers* • *Discouragement from carrying out future business/charity activities* • *Goodwill compensation or discounts given to customers*	**£** **in last <u>12 months</u>**

Appendix B: Interviewer glossary

This is a list of some of the less well-known terms given to interviewers in the quantitative survey to help guide them and respondents. The interviewers had this list to hand before and during interviews. They could read out the definitions here to clarify things if respondents requested this.

Term	Where featured (and page number)	Definition
Business-as-usual health checks vs. ad-hoc health checks or reviews	Q30	Health check activities might include things like staff surveys, security assessments or vulnerability scans. Business-as-usual checks would be activities like this that are undertaken no a scheduled basis, e.g. annually. Ad-hoc checks will be the same kinds of activities but just undertaken as a one-off, e.g. in response to an attack.
Cyber security	Throughout	Cyber security includes any processes, practices or technologies that organisations have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorised access.
Cloud computing	Q32, Q46	Cloud computing uses a network of external servers accessed over the internet, rather than a local server or a personal computer, to store or transfer data. This could be used, for example, to host a website or corporate email accounts, or for storing or transferring data files.
Data classification	Q32	This refers to how files are classified (e.g. public, internal use, confidential etc).
Document Management System	Q32	A Document Management System is a piece of software that can store, manage and track files or documents on an organisation's network. It can help manage things like version control and who has access to specific files or documents.
Externally-hosted web services	Q46	Externally-hosted web services are services run on a network of external servers and accessed over the internet. This could include, for example, services that host websites or corporate email accounts, or for storing or transferring data files over the internet.
GCHQ	Q24 (DO NOT PROMPT)	Government Communications Headquarters – one of the main government intelligence services
GDPR	Q78X, Q78Y, Q78C, Q78D, Q78E, Q78F	The General Data Protection Regulation is a legal framework that sets guidelines for collection and processing of individuals within the European Union (EU).

Term	Where featured (and page number)	Definition
IISP	Q24 (DO NOT PROMPT)	Institute of Information Security Professionals – a security body
Hacking	Q53A, Q64A	Hacking is unauthorised intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose.
Intellectual property	Q21 (DO NOT PROMPT), Q56A, Q75A	Intellectual property (IP) refers to the ideas, data or inventions that are owned by an organisation. This could, for example, include literature, music, product designs, logos, names and images created or bought by the organisation.
ISF	Q24 (DO NOT PROMPT)	Information Security Forum – a security body
Malware	Q31, Q53A, Q64A, Q65, Q68 (DO NOT PROMPT), Q78 (DO NOT PROMPT), Q78F	Malware (short for “malicious software”) is a type of computer program designed to infiltrate and damage computers without the user’s consent (e.g. viruses, worms, Trojan horses etc).
NCSC	Q24 (DO NOT PROMPT)	National Cyber Security Centre – centre set up by Government to issue guidance to businesses and charities, and also support organisations that have been breached
Outsourced provider	Q9C, Q29	Outsourced organisations that deal with an organisation’s cyber security as part of a wider IT support role
Penetration testing	Q78 (DO NOT PROMPT), Q78F	Penetration testing is where staff or contractors try to breach the cyber security of an organisation on purpose, in order to show where there might be weaknesses in cyber security
Personally-owned devices	Q8, Q32, Q67	Personally-owned devices are things such as smartphones, tablets, home laptops, desktop computers or USB sticks that do not belong to the company, but might be used to carry out business-related activities.
Ransomware	Q53A, Q64A	Malicious software that blocks access to a computer system until a sum of money is paid
Removable devices	Q32	Removable devices are portable things that can store data, such as USB sticks, CDs, DVDs etc.
Restricting IT admin and access rights	Q31	Restricting IT admin and access rights is where only certain users are able to make changes to the organisation’s network or computers, for example to download or install software.

Term	Where featured (and page number)	Definition
Risk assessment covering cyber security risks	Q30	This is the process of identifying and controlling any cyber security threats to an organisation's data
Segregated guest wireless networks	Q31	Segregated guest wireless networks are where an organisation allows guests, for example contractors or customers, to access a wi-fi network that is cut off from what staff have access to.
Threat intelligence	Q30	Threat intelligence is where an organisation may employ a staff member or contractor, or purchase a product to collate information and advice around all the cyber security risks the organisation faces.
Two-factor authentication	Q31	This is a type of authentication process were you have to give two bits of information to verify who you are. This might be to access a restricted file, or log into a website or app. For example, it could be a password and another bit of information.

Appendix C: Questionnaire

INTERVIEWER INSTRUCTIONS IN BLUE
ROUTING/SCRIPTING INSTRUCTIONS IN GREEN ITALICS
BUSINESS/CHARITY TEXT SUBSTITUTIONS IN RED (BUSINESS IF SAMPLE TYPE=1, ELSE CHARITY)

Screener

Is this the head office for [SAMPLE 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 Government-sponsored survey on behalf of the Department for Digital, Culture, Media and Sport. It is about how UK [SAMPLE S_TYPE=1: businesses/SAMPLE S_TYPE=2: charities] approach cyber security.

- The purpose is not to sell any software or services. It is conducted annually to generate Official Statistics for the Government.
- We got your contact details from the [SAMPLE S_TYPE=1: Government's Inter-Departmental Business Register/SAMPLE S_COUNTRY=1: Charity Commission for England and Wales/SAMPLE S_COUNTRY=2: Charity Commission for Northern Ireland/SAMPLE S_COUNTRY=3: Office of the Scottish Charity Regulator].
- Taking part is confidential.
- The interview takes an average of 20 minutes, but is typically shorter for smaller organisations.
- We can send you a copy of the findings, as well as a help card with links to Government guidance tailored to [SAMPLE S_TYPE=1: businesses/SAMPLE S_TYPE=2: charities] of your size, as a thank you for taking part.

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

Could I please speak to the senior person at your organisation with the most responsibility when it comes to cyber security?

IF OUTSOURCE CYBER SECURITY: In that case, we want to talk to the person within your organisation who typically deals with an external IT or cyber security provider. We know this may be the business owner, a trustee, Chief Executive, or someone else from the senior management team.

REASSURANCES IF NECESSARY

- The survey helps the Government to understand what guidance organisations like yours need for cyber security. Over the past three years, the findings have led to several improvements to Government guidance.
- The survey is for all types of businesses and charities. We also want to talk to organisations that have not had any cyber security issues, or that outsource their cyber security, so we get your views as well.
- The survey is not technical – we want your views, not just expert opinion on this topic.
- The survey has been endorsed by the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), Tech UK, the Association of British Insurers (ABI),

the Institute of Chartered Accountants in England and Wales (ICAEW), the Charity Commission for England and Wales and the Charity Commission for Northern Ireland.
- To check the survey is legitimate, details of the survey are on the Ipsos MORI website at csbs.ipsos-mori.com. You can also Google the term "Cyber Security Breaches Survey 2019" to find the same link yourself.

REASSURANCE EMAIL SCREEN

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
- 182 – company accountant refusing
- 203 ineligible – sole trader at SIZEA
- 247 ineligible – no computer, website or online use (used very rarely)
- 248 ineligible – public sector at intro
- 249 ineligible – sole trader at intro

READ OUT IF SENDING REASSURANCE EMAIL
This email has more information about the survey plus some text you can type into Google to find our website. The website gives examples of the kinds of questions we ask. I strongly recommend looking at it before taking part. Other participants have told us it is helpful to see the main questions in advance, so they can get the answers ready before the interview.

Consent

ASK ALL
Q1A.CONSENT
Before we start, I just want to clarify that participation in the survey is voluntary and you can change your mind at any time. Are you happy to proceed with the interview?

Yes
No *CLOSE SURVEY*

Business profile

Q1.DELETED POST-PILOT IN 2016 SURVEY

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

Q2.DELETED POST-PILOT IN 2016 SURVEY

Q3.DELETED POST-PILOT IN 2016 SURVEY

ASK IF BUSINESS (SAMPLE TYPE=1)
Q5X.TYPEX
Would you classify your organisation as … ?
READ OUT
INTERVIEWER NOTE: IF THEY HAVE A SOCIAL PURPOSE BUT STILL MAKE A PROFIT (E.G. PRIVATE PROVIDER OF HEALTH OR SOCIAL CARE) CODE AS CODE 1

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

DUMMY VARIABLE NOT ASKED
Q5Y.TYPEXDUM
Would you classify your organisation as … ?

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

SCRIPT TO BASE [BUSINESS/CHARITY] TEXT SUBSTITUTIONS ON TYPEXDUM (CHARITY IF TYPEXDUM CODE 2, ELSE BUSINESS). THIS IS THE DEFAULT SCRIPTING FOR ALL TEXT SUBSTITUTIONS FROM THIS POINT ONWARDS, UNLESS OTHERWISE SPECIFIED.

ASK ALL
Q4.SIZEA
Including yourself, how many [employees/employees, volunteers and trustees] work for 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. / By that I mean both full-time and part-time employees on your payroll, as well as people who regularly volunteer for your organisation.]
PROBE FOR BEST ESTIMATE BEFORE CODING DK

Respondent is sole trader *THANK AND CLOSE (CLOSE SURVEY)*
WRITE IN RANGE 2–500,000
(SOFT CHECK IF >99,999; ALLOW DK)

ASK IF DON'T KNOW SIZE OF ORGANISATION (SIZEA CODE DK)
Q5.SIZEB
Which of these best represents the number of [employees/employees, volunteers and trustees] working for your organisation across the UK as a whole, including yourself?
PROBE FULLY

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

DUMMY VARIABLE NOT ASKED
Q5X.SIZEDUM
Which of these best represents the number of employees, volunteers and trustees working in your organisation, including yourself?

Under 10
10–49
50–249
IF SIZEB CODES 4–5: 250 or more
Don't know
(SINGLE CODE; MERGE RESPONSES FROM SIZEA AND SIZEB; USE SAMPLE S_SIZEBAND IF SIZEB DK)

ASK IF NO INCOME RECORDED IN SAMPLE (SAMPLE S_INCOMEBAND BLANK)
Q5A.SALESA
In the financial year just gone, [what was the approximate turnover of your organisation across the UK as a whole? / what was the approximate total income of your charity across the UK as a whole?]
ADD IF NECESSARY: [The total amount received in respect of sales of goods and services. / *The total amount of donations or other funds raised.]*
PROBE FOR BEST ESTIMATE BEFORE CODING DK
ADD IF NECESSARY: This will help us to better understand the rest of the answers you give in the survey. As with the rest of the questions, all your responses are totally confidential.

WRITE IN RANGE £0+
(SOFT CHECK IF <£1,000 OR >£50,000,000; ALLOW DK OR REF)

ASK IF DON'T KNOW NUMERIC TURNOVER OF ORGANISATION (SALESA CODE DK)
Q5B.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
PROBE FOR BEST ESTIMATE BEFORE CODING DK

Less than £10,000
£10,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £5 million
£5 million to less than £10 million
£10 million to less than £50 million
£50 million or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

DUMMY VARIABLE NOT ASKED
Q5Z.SALESDUM
Which of these best represents the turnover or income of your organisation across the UK as a whole in the financial year just gone?

Less than £10,000
£10,000 to less than £100,000

£100,000 to less than £500,000
£500,000 to less than £5 million
£5 million to less than £10 million
£10 million to less than £50 million
£50 million or more
Don't know
Refused
(SINGLE CODE; MERGE RESPONSES FROM SALESA AND SALESB)

Q5C.YEARS DELETED POST-PILOT IN 2018 SURVEY

Q5D.CHARITYO DELETED PRE-PILOT IN 2019 SURVEY

ASK ALL
Q6.ONLINE
Which of the following, if any, does your organisation currently have or use?
READ OUT

Email addresses for your organisation or its [employees/*employees or volunteers]*
A website or blog
Accounts or pages on social media sites (e.g. Facebook or Twitter)
The ability for customers to order, book or pay for products or services online
ONLY SHOW IF CHARITY: The ability for people to donate online
ONLY SHOW IF CHARITY: The ability for your beneficiaries or service users to access services online
An online bank account your organisation or your clients pay into
ONLY SHOW IF SAMPLE SICVAR=1: An industrial control system
Personal information about your [*customers/beneficiaries, service users or donors]* held electronically
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES)

Q7.CORE DELETED PRE-PILOT IN 2019 SURVEY

ASK ALL
Q8.MOBILE
As far as you know, does anyone in your organisation use personally-owned devices, such as smartphones, tablets, home laptops or desktop computers to carry out regular business-related activities, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

Perceived importance and preparedness

READ OUT TO ALL
For the rest of the survey, I will be talking about cyber security. By this, I mean any strategy, processes, practices or technologies that organisations have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorised access.

ASK ALL
Q9.PRIORITY

How high or low a priority is cyber security to your organisation's [INSERT STATEMENT]? Is it ...
READ OUT

a. [Directors/trustees] or senior management
b. DELETED DURING FIELDWORK IN 2018 SURVEY
c. DELETED DURING FIELDWORK IN 2018 SURVEY

Very high
Fairly high
Fairly low
Very low
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT TO ROTATE STATEMENTS b AND c ONLY; REVERSE SCALE EXCEPT FOR LAST CODE)

Q9A.HIGH DELETED POST-PILOT IN 2017 SURVEY

Q9B.RELPRIORITY DELETED POST-PILOT IN 2018 SURVEY

ASK ALL
Q9C.OUTSOURCE
Which of the following best represents your organisation when it comes to outsourcing cyber security to external organisations or individuals? This can include organisations or individuals that deal with your cyber security as part of a wider IT support role.
READ OUT

We have an outsourced provider that manages our cyber security
We do not have an outsourced provider, but intend to use one
We do not have an outsourced provider and do not intend to use one
DO NOT READ OUT: Don't know
(SINGLE CODE)

Q10.LOW DELETED PRE-PILOT IN 2018 SURVEY

ASK ALL
Q10A.ATTITUDES
How much do you agree or disagree with the following statements?
READ OUT

a. **NOT USED**
b. **NOT USED**
c. **NOT USED**
d. **NOT USED**
e. The people dealing with cyber security in our organisation have the right cyber security skills and knowledge to do this job effectively
f. We have enough people dealing with cyber security in our organisation to effectively manage the risks
g. I am not sure how our organisation should act on any advice I have seen or heard around cyber security

h. *ONLY SHOW IF HAVE OUTSOURCED OR INTEND TO OUTSOURCE (OUSOURCE CODES 1–2):* We have the knowledge and understanding we need to make an informed choice between outsourced cyber security providers

Strongly agree
Tend to agree
Neither agree nor disagree
Tend to disagree
Strongly disagree
DO NOT READ OUT: Don't know
SHOW FOR ATTITUDESg: DO NOT READ OUT: Have not seen or heard anything about cyber security
(SINGLE CODE; SCRIPT TO ROTATE STATEMENTS BUT KEEP e BEFORE f AND REVERSE SCALE EXCEPT FOR LAST CODE)

Q10B.LOWRISK REMOVED POST-PILOT IN 2017 SURVEY

ASK ALL
Q11.UPDATE
Approximately how often, if at all, are your organisation's [directors/trustees] or senior management given an update on any actions taken around cyber security? Is it …
READ OUT

Never
Less than once a year
Annually
Quarterly
Monthly
Weekly
Daily
DO NOT READ OUT: Each time there is a breach or attack
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST 2 CODES)

Spending

ASK ALL
Q11A.MICROSITE
We have a page on the Ipsos MORI website to help you answer some of the questions and make the survey quicker. The webpage doesn't ask you to enter any information or download anything. Do you have a smartphone or computer to go to this webpage now, and have it open for the rest of the survey?

The link is csbs.ipsos-mori.com and you need to click on the "During interview" tab at the top.

ADD IF NECESSARY: We can finish the survey without it, but other organisations have told us that having it open makes the survey quicker for them.

Yes
No
(SINGLE CODE)

ASK ALL
Q12.INVESTA
[IF USING MICROSITE (MICROSITE CODE 1): For this next question, you can click on the "investment in cyber security" box on the website for some helpful guidance.]
In the financial year just gone, approximately how much, if anything, did you invest in cyber security? By this, I mean spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please **do not** include any spending you have undertaken to repair or recover from breaches or attacks.

To make it easiest for you, would you like to answer…?
READ OUT
INTERVIEWER NOTE: THIS WAS ON THE PRE-INTERVIEW QUESTIONS SHEET
INTERVIEWER NOTE: IF UNABLE TO CHOOSE, SELECT CODE 1
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

As a number in £s
ONLY SHOW IF GIVES TURNOVER (SALESDUM CODES 1–7 OR SAMPLE S_INCOMEBAND NOT BLANK): As a percentage of [turnover/your organisation's income]
Or as a percentage of overall IT expenditure
DO NOT READ OUT: Don't invest anything
DO NOT READ OUT: Refused
(SINGLE CODE)

ASK IF ANSWERING AS A NUMBER (INVESTA CODE 1)
Q13.INVESTB
How much, if anything, was it as a number in £s?
REMIND IF NECESSARY: Please include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please do not include any spending on personal IT equipment or its software.
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL IF DON'T INVEST ANYTHING

WRITE IN RANGE £1–£99,999,999
IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2): (SOFT CHECK IF <£100 OR >£99,999; ALLOW DK AND NULL)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£1,000 OR >£999,999; ALLOW DK AND NULL)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£9,999,999; ALLOW DK AND NULL)

ASK IF DON'T KNOW TOTAL NUMERIC INVESTMENT IN CYBER SECURITY (INVESTB CODE DK)
Q14.INVESTC
Was it approximately...?
REMIND IF NECESSARY: Please include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please do not include any spending on personal IT equipment or its software.
PROBE FULLY

IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2):
Less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 or more
DO NOT READ OUT: Don't know
DO NOT READ OUT: Don't invest anything

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3):
Less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million or more
DO NOT READ OUT: Don't know
DO NOT READ OUT: Don't invest anything

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]):
Less than £10,000
£10,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million to less than £10 million
£10 million or more
DO NOT READ OUT: Don't know
DO NOT READ OUT: Don't invest anything
(SINGLE CODE)

ASK IF ANSWERING AS A PERCENTAGE OF TURNOVER (INVESTA CODE 2)
Q15.INVESTD
How much, if anything, was it as a percentage of turnover?
REMIND IF NECESSARY: Please include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please do not include any spending on personal IT equipment or its software.
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL IF SPENT SOMETHING, BUT LESS THAN 1%

WRITE IN RANGE 0%–100%
(SOFT CHECK IF >19%; ALLOW DK AND NULL)

ASK IF DON'T KNOW INVESTMENT IN CYBER SECURITY AS A SPECIFIC PERCENTAGE OF TURNOVER (INVESTD CODE DK)

Q16.INVESTE
Was it approximately... ?
REMIND IF NECESSARY: Please include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please do not include any spending on personal IT equipment or its software.
PROBE FULLY

Less than 1%
1% to 2%
3% to 4%
5% to 9%
10% to 14%
15% to 19%
20% or more
DO NOT READ OUT: Don't know
DO NOT READ OUT: Don't invest anything
(SINGLE CODE)

ASK IF ANSWERING AS A PERCENTAGE OF OVERALL IT EXPENDITURE (INVESTA CODE 3)
Q17.INVESTF
How much, if anything, was it as a percentage of overall IT expenditure?
REMIND IF NECESSARY: Please include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please do not include any spending on personal IT equipment or its software.
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL IF SPENT SOMETHING, BUT LESS THAN 1%

WRITE IN RANGE 0%–100%
(SOFT CHECK IF >74%; ALLOW DK AND NULL)

ASK IF DON'T KNOW INVESTMENT IN CYBER SECURITY AS A SPECIFIC PERCENTAGE OF OVERALL IT EXPENDITURE (INVESTF CODE DK)
Q18.INVESTG
Was it approximately ... ?
REMIND IF NECESSARY: Please include spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. Please do not include any spending on personal IT equipment or its software.
PROBE FULLY

Under 5%
5% to 9%
10% to 24%
25% to 49%
50% to 74%
75% or more
DO NOT READ OUT: Don't know
DO NOT READ OUT: Don't invest anything
(SINGLE CODE)

ASK IF ANSWERING AS A PERCENTAGE OF OVERALL IT EXPENDITURE AND INVEST IN CYBER SECURITY (INVESTF CODE>0 OR NULL OR INVESTG CODES 1–6)

Q19.ITA

And in the financial year just gone, how much was your total IT expenditure?
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE £1–£99,999,999
IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2): (SOFT CHECK IF <£100 OR >£99,999; ALLOW DK)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£1,000 OR >£999,999; ALLOW DK)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£50,000,000; ALLOW DK)

ASK IF DON'T KNOW TOTAL NUMERIC IT EXPENDITURE (ITA CODE DK)

Q20.ITB

Was it approximately ... ?
PROBE FULLY

IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2):
Less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £250,000
£250,000 to less than £500,000
£500,000 or more
DO NOT READ OUT: Don't know

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3):
Less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £250,000
£250,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million or more
DO NOT READ OUT: Don't know

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]):
Less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million to less than £10 million
£10 million to less than £20 million
£20 million or more
DO NOT READ OUT: Don't know

(SINGLE CODE)

ASK IF INVEST IN CYBER SECURITY (INVESTB CODE>0 OR INVESTC CODES 1–7 OR INVESTD CODE>0 OR NULL OR INVESTE CODES 1–7 OR INVESTF CODE>0 OR NULL OR INVESTG CODES 1–6)

Q21.REASON

What are the main reasons that your organisation invests in cyber security?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")
INTERVIEWER NOTE: IF "PROTECTION IN GENERAL/TO SECURE OURSELVES/PREVENT BREACHES/ATTACKS", PROBE WHY THEY FEEL THEY HAVE TO DO THIS

Business continuity/keeping the organisation running
Clients/customers/beneficiaries/service users/donors require it
Complying with laws/regulations
Government cyber security initiatives
Improving efficiency/reducing costs
Media/press coverage of topic/breaches/attacks
Preventing downtime and outages
Preventing fraud/theft
Protecting trade secrets/intellectual property
Protecting customer/beneficiary/service user/donor information/data
Protecting other assets (e.g. cash)
Protecting the organisation's reputation/brand
Suffered cyber security breach/attack previously
Other *WRITE IN*
(MULTICODE; ALLOW DK)

Q22.EVAL DELETED PRE-PILOT IN 2018 SURVEY

Q23.INSURE DELETED PRE-PILOT IN 2018 SURVEY

READ OUT TO ALL

Now I would like to ask some questions about measures you may or may not have taken around cyber security. Just to reassure you, we are not looking for a "right" or "wrong" answer at any question.

ASK ALL

Q23X.INSUREX

There are specific insurance policies, separate from general liability insurance, that can cover organisations in the event of a breach or attack. These are sometimes called cyber security insurance, cyber risk insurance, or cyber liability insurance. When it comes to these types of insurance, which of the following best describes your situation?
READ OUT

We have a specific cyber security insurance policy
We do not currently have a specific cyber security insurance policy, but have previously considered it
We do not currently have a specific cyber security insurance policy and have not previously considered it
DO NOT READ OUT: Don't know
(SINGLE CODE)

Q23A.COVERAGE DELETED PRE-PILOT IN 2018 SURVEY

ASK IF HAVE INSURANCE (INSUREX CODE 1)
Q23B.CLAIM
Have you ever made any insurance claims for cyber security breaches under this insurance before?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF DO NOT HAVE INSURANCE (INSUREX CODES 2–3)
Q23C.NOINSURE
As far as you know what are the reasons why your organisation has not taken out a specific cyber security insurance policy?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")

Don't think they need it
Can't see the benefits/need
Covered by another/general insurance policy
Covered externally/through an outsourced provider
Cyber attack would not impact us much
Don't consider ourselves at risk/low risk
Existing measures good enough
We are too small/insignificant size

Issues with current policies/products
Available policies are confusing
Available policies have restrictive conditions
Available policies not right for our organisation generally
Market too new/undeveloped
Not affordable/costs too much/high premiums
Offers insufficient coverage

Not aware/not considered enough
Aware but have not prioritised it/weighed it up
Intend to get it/still looking
Not aware of it/thought about it before

Other WRITE IN
(MULTICODE; ALLOW DK)

Information sources

ASK ALL
Q24.INFO
In the last 12 months, from where, if anywhere, have you sought information, advice or guidance on the cyber security threats that your organisation faces?
DO NOT READ OUT
INTERVIEWER NOTE: IF "GOVERNMENT", THEN PROBE WHERE EXACTLY
PROBE FULLY ("ANYWHERE ELSE?")

CODE NULL FOR "NOWHERE"

Government/public sector
Government's 10 Steps to Cyber Security guidance
Government's Cyber Aware website/materials
Government's Cyber Essentials materials
Government intelligence services (e.g. GCHQ)
GOV.UK/Government website (excluding NCSC website)
Government – other *WRITE IN*
National Cyber Security Centre (NCSC) website/offline
Police
Regulator (e.g. Financial Conduct Authority) – but excluding Charity Commission

Charity related
Association of Chief Executives of Voluntary Organisations (ACEVO)
Charity Commission (England and Wales, Scotland or Northern Ireland)
Charity Finance Group (CFG)
Community Accountants
Community Voluntary Services (CVS)
Institute of Fundraising (IOF)
National Council For Voluntary Organisations (NCVO)
Other local infrastructure body
Other national infrastructure body

Other specific organisations
Cyber Security Information Sharing Partnership (CISP)
Professional/trade/industry/volunteering association
Security bodies (e.g. ISF or IISP)
Security product vendors (e.g. AVG, Kaspersky etc)

Internal
Within your organisation – senior management/board
Within your organisation – other colleagues or experts

External
Auditors/accountants
Bank/business bank/bank's IT staff
External security/IT consultants/cyber security providers
Internet Service Provider
LinkedIn
Newspapers/media
Online searching generally/Google
Specialist IT blogs/forums/websites
Other (non-government) *WRITE IN*
(MULTICODE; ALLOW DK AND NULL)

Q24A.FINDING DELETED POST-PILOT IN 2017 SURVEY

ASK IF SOUGHT GOVERNMENT INFORMATION (INFO CODES 1-7)
Q24B.GOVTINF
From what you know or have heard, how useful, if at all, is the information, advice or guidance on cyber security that comes from the Government for organisations like yours?

READ OUT

Very useful
Fairly useful
Not very useful
Not at all useful
DO NOT READ OUT: Don't know
DO NOT READ OUT: Not aware of anything from the Government on cyber security
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST CODE)

ASK ALL
Q24C.CYBERAWARE
And have you heard of or seen the Cyber Aware campaign, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

Training

Q25. DELETED POST-PILOT IN 2016 SURVEY

ASK ALL
Q26.TRAIN
Over the last 12 months, have you or anyone from your organisation done any of the following, or not?
READ OUT

Attended seminars or conferences on cyber security
Attended any externally-provided training on cyber security
Received any internal training on cyber security
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES)

READ OUT IF SEMINARS OR TRAINING ATTENDED (TRAIN CODES 1–3)
I now want to ask about all the internal or external cyber security training, seminars or conferences attended over the last 12 months.

Q26A.TRAINUSE DELETED POST-PILOT IN 2017 SURVEY

ASK IF SEMINARS OR TRAINING ATTENDED (TRAIN CODES 1–3)
Q26B.TRAINWHO
Who in your organisation attended any of the training, seminars or conferences over the last 12 months?
PROMPT TO CODE

[Directors/trustees] or senior management
IT staff
Staff members whose job role includes information security or governance
Other staff who are not cyber security or IT specialists
ONLY SHOW IF CHARITY: Volunteers

DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE)

Q27.DELIVER DELETED POST-PILOT IN 2018 SURVEY

Q28.COVER DELETED POST-PILOT IN 2017 SURVEY

Policies and procedures

READ OUT TO ALL
Now I would like to ask some questions about processes and procedures to do with cyber security. Again, just to reassure you, we are not looking for a "right" or "wrong" answer at any question.

ASK ALL
Q29.MANAGE
Which of the following governance or risk management arrangements, if any, do you have in place?
READ OUT

[Board members*/trustees]* with responsibility for cyber security
An outsourced provider that manages your cyber security
A formal policy or policies in place covering cyber security risks
A Business Continuity Plan
Staff members whose job role includes information security or governance
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES)

ASK IF DO NOT HAVE GOVERNANCE OR RISK MANAGEMENT ARRANGEMENTS (MANAGE CODES 7 OR DK)
Q29B.NOPOL
You said that you do not have any of the governance or risk management arrangements that I mentioned in place. What are the reasons for not having these?
DO NOT READ OUT
INTERVIEWER NOTE: IF "DON'T HAVE THE RESOURCES", THEN PROBE WHAT RESOURCES (E.G. TIME, COST ETC)
PROBE FULLY ("ANYTHING ELSE?")

Can't recruit right staff/skills
Cost/too expensive
Don't consider cyber security a risk/significant risk
Don't have time to arrange/set up
Too complex to arrange/set up
Don't hold commercially valuable information
Don't hold customer/beneficiary/service user/donor data
Don't hold financial data (e.g. credit card details)
Don't hold politically sensitive information
Don't offer services/carry out transactions online
In the process of setting up arrangements
Manage it informally/don't need formal arrangements

Not important/a priority
Small organisation/insignificant size
Have something else in place
Won't make a difference/can't see benefits
Other *WRITE IN*
(MULTICODE; ALLOW DK)

ASK ALL
Q30.IDENT
And which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation?
READ OUT

An internal audit
An external audit
Any business-as-usual health checks that are undertaken regularly
Ad-hoc health checks or reviews beyond your regular processes
A risk assessment covering cyber security risks
Invested in threat intelligence
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES, AND CODE 4 MUST FOLLOW CODE 3)

ASK ALL
Q31.RULES
And which of the following rules or controls, if any, do you have in place?
READ OUT

Applying software updates when they are available
Up-to-date malware protection
Firewalls with appropriate configuration
Restricting IT admin and access rights to specific users
Any monitoring of user activity
Specific rules for storing and moving personal data files securely
Security controls on company-owned devices (e.g. laptops)
Only allowing access via company-owned devices
A segregated guest wireless network
Two-factor authentication to access restricted files, or log into your own websites or apps
Backing up data securely via a cloud service
Backing up data securely via other means
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES AND KEEP CODES 11 AND 12 TOGETHER)

ASK IF HAVE POLICIES (MANAGE CODE 3)
Q32.POLICY
Which of the following aspects, if any, are covered within your cyber security-related policy, or policies?
READ OUT

What can be stored on removable devices (e.g. USB sticks, CDs etc)
Remote or mobile working (e.g. from home)
What staff are permitted to do on your organisation's IT devices
Use of personally-owned devices for business activities
Use of new digital technologies such as cloud computing
Data classification
A Document Management System
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES)

Q32A.FOLLOW DELETED POST-PILOT IN 2017 SURVEY

Q33.DOC DELETED PRE-PILOT IN 2019 SURVEY

ASK IF HAVE ANY POLICIES (MANAGE CODE 3)
Q33A.REVIEW
When were any of your policies or documentation for cyber security last created, updated, or reviewed to make sure they were up-to-date?
PROBE FULLY
INTERVIEWER NOTE: IF NEVER UPDATED OR REVIEWED, ANSWER IS WHEN POLICIES WERE CREATED

Within the last 6 months
6 to under 12 months ago
12 to under 24 months ago
24 months ago or earlier
DO NOT READ OUT: Don't know
(SINGLE CODE)

Business standards

Q34.ISO DELETED DURING FIELDWORK IN 2018 SURVEY

Q35.IMPLEMA DELETED DURING FIELDWORK IN 2018 SURVEY

ASK IF NOT ALREADY MENTIONED 10 STEPS AS AN INFORMATION SOURCE (INFO NOT CODE 1)
Q36.TENSTEPS
Are you aware of the Government's 10 Steps to Cyber Security guidance, or not?

Yes
No
(SINGLE CODE; DP AUTO-CODE 1 IF INFO CODE 1; ALLOW DK)

ASK ALL
Q37.ESSENT
And are you aware of the Government-backed Cyber Essentials scheme, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF AWARE OF CYBER ESSENTIALS (ESSENT CODE 1)
Q38.IMPLEMB
Has your organisation done any of the following, or not?
READ OUT

Fully implemented Cyber Essentials, but not Cyber Essentials Plus
Fully implemented Cyber Essentials Plus
Partially implemented Cyber Essentials
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(SINGLE CODE)

Q39. DELETED PRE-PILOT IN 2017 SURVEY

Q40. DELETED PRE-PILOT IN 2017 SURVEY

Q41. DELETED PRE-PILOT IN 2017 SURVEY

Q42. DELETED PRE-PILOT IN 2016 SURVEY

Q43. DELETED PRE-PILOT IN 2016 SURVEY

Supplier standards

ASK ALL
Q44.SUPPLY
Do you currently require your suppliers to have or adhere to any cyber security standards or good practice guides, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF HAVE SUPPLIER STANDARDS (SUPPLY CODE 1)
Q45.ADHERE
Which of the following, if any, do you require your suppliers to have or adhere to?
READ OUT

A recognised standard such as ISO 27001
Payment Card Industry Data Security Standard (PCI DSS)
An independent service auditor's report (e.g. ISAE 3402)
ONLY SHOW IF ESSENT CODE 1: Cyber Essentials
ONLY SHOW IF ESSENT CODE 1: Cyber Essentials Plus
Any other standards or good practice guides
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 3 CODES)

Cloud computing

ASK ALL
Q46.CLOUD

Does your organisation currently use any externally-hosted web services, for example to host your website or corporate email accounts, or for storing or transferring data?
ADD IF NECESSARY: Examples of these kinds of cloud service include Microsoft Office Online and Apple iCloud.

Yes
No
(SINGLE CODE; ALLOW DK)

Q47. DELETED POST-PILOT IN 2016 SURVEY

Q48.CRITICAL DELETED POST-PILOT IN 2017 SURVEY

Q49.COMMER DELETED PRE-PILOT IN 2018 SURVEY

Q50.PERSON DELETED PRE-PILOT IN 2018 SURVEY

Q51.VALIDA DELETED POST-PILOT IN 2017 SURVEY

Q52.VALIDB DELETED POST-PILOT IN 2017 SURVEY

Breaches or attacks

READ OUT TO ALL
Now I would like to ask some questions about cyber security breaches or attacks. *[IF MANAGE CODE 2:* I understand that breaches or attacks may be dealt with directly by your outsourced provider, so please answer what you can, based on what you know.*]*

Q53. DELETED PRE-PILOT IN 2017 SURVEY

ASK ALL
Q53A.TYPE
Have any of the following happened to your organisation in the last 12 months, or not?
READ OUT
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

Computers becoming infected with ransomware
Computers becoming infected with other viruses, spyware or malware
ONLY SHOW IF ONLINE CODE 2: Attacks that try to take down your website or online services
Hacking or attempted hacking of online bank accounts
People impersonating your organisation in emails or online
Staff receiving fraudulent emails or being directed to fraudulent websites
Unauthorised use of computers, networks or servers by staff, even if accidental
Unauthorised use or hacking of computers, networks or servers by people outside your organisation
Any other types of cyber security breaches or attacks
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
DO NOT READ OUT: Refused
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 4 CODES, AND CODE 2 MUST FOLLOW CODE 1)

ASK IF ANY BREACHES OR ATTACKS (TYPE CODES 1–9)

Q54.FREQ

Approximately, how often in the last 12 months did you experience any of the cyber security breaches or attacks you mentioned? Was it …

READ OUT

REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

Once only
More than once but less than once a month
Roughly once a month
Roughly once a week
Roughly once a day
Several times a day
DO NOT READ OUT: Don't know
DO NOT READ OUT: Refused
(SINGLE CODE)

ASK IF EXPERIENCED BREACHES OR ATTACKS MORE THAN ONCE (FREQ CODES 2–6 OR DK)

Q55.NUMBA

And approximately, how many breaches or attacks have you experienced **in total** across the last 12 months?

PROBE FOR BEST ESTIMATE BEFORE CODING DK

REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

IF FREQ CODES 2–3 OR DK: WRITE IN RANGE 2–1,000,000
IF FREQ CODES 4–5: WRITE IN RANGE 25–1,000,000
IF FREQ CODE 6: WRITE IN RANGE 200–1,000,000
(SOFT CHECK IF >99,999; DP AUTO-CODE 1 IF FREQ CODE 1; ALLOW DK AND REF)

ASK IF DON'T KNOW HOW MANY BREACHES OR ATTACKS EXPERIENCED (NUMBA CODE DK)

Q56.NUMBB

Was it approximately ... ?

PROBE FULLY

IF BREACHED OR ATTACKED LESS THAN ONCE A MONTH OR DON'T KNOW (FREQ CODE 2 OR DK)

Fewer than 3
3 to fewer than 5
5 to fewer than 10
10 to fewer than 15
15 to fewer than 20
20 or more
DO NOT READ OUT: Don't know

IF BREACHED OR ATTACKED ONCE A MONTH (FREQ CODE 3)

Fewer than 15
15 to fewer than 20
20 to fewer than 25
25 or more
DO NOT READ OUT: Don't know

IF BREACHED OR ATTACKED ONCE A WEEK (FREQ CODE 4)
Fewer than 50
50 to fewer than 75
75 to fewer than 100
100 or more
DO NOT READ OUT: Don't know

IF BREACHED OR ATTACKED ONCE A DAY (FREQ CODE 5)
Fewer than 100
100 to fewer than 200
200 to fewer than 300
300 to fewer than 400
400 to fewer than 500
500 or more
DO NOT READ OUT: Don't know

IF BREACHED OR ATTACKED SEVERAL TIMES A DAY (FREQ CODE 6)
Fewer than 500
500 to fewer than 750
750 to fewer than 1,000
1,000 to fewer than 5,000
5,000 to fewer than 10,000
10,000 to fewer than 100,000
100,000 or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK IF ANY BREACHES OR ATTACKS (TYPE CODES 1–9)
Q56A.OUTCOME
Thinking of all the cyber security breaches or attacks experienced in the last 12 months, which, if any, of the following happened as a result?
READ OUT

Software or systems were corrupted or damaged
Personal data *(e.g. on [customers or staff/beneficiaries, donors, volunteers or staff])* was altered, destroyed or taken
Permanent loss of files (other than personal data)
Temporary loss of access to files or networks
Lost or stolen assets, trade secrets or intellectual property
Money was stolen
ONLY SHOW IF ONLINE CODE 2: Your website or online services were taken down or made slower
Lost access to any third-party services you rely on
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES, CODE 4 MUST FOLLOW CODE 3)

ASK IF ANY BREACHES OR ATTACKS (TYPE CODES 1–9)
Q57.IMPACT

And have any of these breaches or attacks impacted your organisation in any of the following ways, or not?
READ OUT

Stopped staff from carrying out their day-to-day work
Loss of [revenue or share value/income]
Additional staff time to deal with the breach or attack, or to inform [customers/beneficiaries] or stakeholders
Any other repair or recovery costs
New measures needed to prevent or protect against future breaches or attacks
Fines from regulators or authorities, or associated legal costs
Reputational damage
Prevented provision of goods or services to [customers/beneficiaries or service users]
Discouraged you from carrying out a future business activity you were intending to do
Complaints from [customers/beneficiaries or stakeholders]
Goodwill compensation or discounts given to customers
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES, AND CODE 4 MUST FOLLOW CODE 3)

Q58.MONITOR DELETED PRE-PILOT IN 2018 SURVEY

ASK IF ANY BREACHES OR ATTACKS (TYPE CODES 1–9)
Q59.COSTA
[IF USING MICROSITE (MICROSITE CODE 1): For this next question, you can click on the "cost of cyber security breaches or attacks" box on the website for some helpful guidance.]
Approximately how much, if anything, do you think the cyber security breaches or attacks you have experienced in the last 12 months have cost your organisation financially? This includes any of the direct and indirect costs or damages you mentioned earlier [IF USING MICROSITE (MICROSITE CODE 1): and which are listed on the website].
INTERVIEWER NOTE: THIS WAS ON THE PRE-INTERVIEW QUESTIONS SHEET
PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
CODE NULL FOR NO COST INCURRED

WRITE IN RANGE £1–£30,000,000
IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2): (SOFT CHECK IF >£99,999; ALLOW DK, NULL AND REF)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£999,999; ALLOW DK, NULL AND REF)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999; ALLOW DK, NULL AND REF)

ASK IF DON'T KNOW TOTAL COST OF CYBER SECURITY BREACHES OR ATTACKS (COSTA CODE DK)
Q60.COSTB
Was it approximately ... ?
PROBE FULLY

IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2):
Less than £500

£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 or more
DO NOT READ OUT: Don't know

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3):
Less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 or more
DO NOT READ OUT: Don't know

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]):
Less than £1000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

Q61. DELETED POST-PILOT IN 2016 SURVEY

Q62. DELETED PRE-PILOT IN 2017 SURVEY

ASK ALL
Q63.INCID
Do you have any formal cyber security incident management processes, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

Most disruptive breach or attack

READ OUT IF MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE TYPE CODES 1–9)

Now I would like you to think about the one cyber security breach, or related series of breaches or attacks, that caused the most disruption to your organisation in the last 12 months.

Q64. DELETED PRE-PILOT IN 2017 SURVEY

ASK IF MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE TYPE CODES 1–9)
Q64A.DISRUPTA
What kind of breach was this?
PROMPT TO CODE IF NECESSARY
INTERVIEWER NOTE: IF MORE THAN ONE CODE APPLIES, ASK RESPONDENT WHICH ONE OF THESE THEY THINK STARTED OFF THE BREACH OR ATTACK

Computers becoming infected with ransomware
Computers becoming infected with other viruses, spyware or malware
Attacks that try to take down your website or online services
Hacking or attempted hacking of online bank accounts
People impersonating your organisation in emails or online
Staff receiving fraudulent emails or being directed to fraudulent websites
Unauthorised use of computers, networks or servers by staff, even if accidental
Unauthorised use or hacking of computers, networks or servers by people outside your organisation
Any other types of cyber security breaches or attacks
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT ONLY SHOW CODES MENTIONED AT TYPE; DP AUTO-CODE SAME CODE FROM TYPE IF ONLY 1 CODE MENTIONED)

READ OUT IF EXPERIENCED ONE TYPE OF BREACH OR ATTACKS MORE THAN ONCE ([ONLY 1 TYPE CODES 1–9] AND [FREQ CODES 2–6 OR DK])
You mentioned you had experienced *[INSERT RESPONSE FROM TYPE]* on more than one occasion. Now I would like you to think about the one instance of this that caused the most disruption to your organisation in the last 12 months.

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)
Q65.IDENTB
IF ONE TYPE OF BREACH OR ATTACK EXPERIENCED ONLY ONCE ([ONLY 1 TYPE CODES 1–9] AND FREQ CODE 1): Now thinking again about the one cyber security breach or attack you mentioned having in the last 12 months, how was this breach or attack identified?
IF MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF EXPERIENCED BREACHES OR ATTACKS MORE THAN ONCE ([2 OR MORE TYPE CODES 1–9] OR [FREQ CODES 2–6 OR DK]): How was the breach or attack identified in this particular instance?
IF ONE TYPE OF BREACH OR ATTACK EXPERIENCED (ONLY 1 TYPE CODES 1–9):
PROMPT IF NECESSARY WITH BREACH OR ATTACK MENTIONED EARLIER: *[INSERT RESPONSE FROM TYPE]*
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")
CODE NULL FOR NONE OF THESE

By accident
By antivirus/anti-malware software

Disruption to business/staff/users/service provision
From warning by government/law enforcement
Our breach/attack reported by the media
Similar incidents reported in the media
Reported/noticed by customer(s)/beneficiaries/service users/donors/customer complaints
Reported/noticed by staff/contractors/volunteers
Routine internal security monitoring
Other internal control activities not done routinely (e.g. reconciliations, audits etc)
Other *WRITE IN*
(MULTICODE; ALLOW DK AND NULL)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q66.LENGTH

As far as you know, how long was it, if any time at all, between this breach or attack occurring and it being identified as a breach? Was it …
PROBE FULLY

Immediate
Within 24 hours
Within a week
Within a month
Within 100 days
Longer than 100 days
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q67.FACTOR

As far as you know, what factors contributed to this breach or attack occurring?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")

Antivirus/other software out-of-date/unreliable/not updated
External attack specifically targeted at your organisation
External attack **not** specifically targeted at your organisation
Human error
Passwords not changed/not secure enough
Policies/processes poorly designed/not effective
Necessary policies/processes not in place
Politically motivated breach or attack
Portable media bypassed defences
Staff/ex-staff/contractors deliberately abusing their account
Staff/ex-staff/contractors not adhering to policies/processes
Staff/ex-staff/contractors not vetted/not vetted sufficiently
From staff/contractors' personally-owned devices (e.g. USB sticks, smartphones etc)
Staff lacking awareness/knowledge
Unsecure settings on browsers/software/computers/user accounts
Visiting untrusted/unsafe websites/pages

Weaknesses in someone else's security (e.g. suppliers)
Other *WRITE IN*
(MULTICODE; ALLOW DK)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q68.SOURCE
As far as you know, who or what was the source of the breach or attack?
DO NOT READ OUT
INTERVIEWER NOTE: IF VIRUS/MALWARE, PROBE WHERE THEY THINK THIS CAME FROM
PROBE FULLY ("ANYONE ELSE?")

3rd party supplier(s)
Activists
Competitor(s)
Emails/email attachments/websites
Employee(s)/volunteers
Former employee(s)/volunteers
Malware author(s)
Nation-state intelligence services
Natural (flood, fire, lightening etc)
Non-professional hacker(s)
Organised crime
Terrorists
Other *WRITE IN*
(MULTICODE; ALLOW DK)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q69.INTENT
As far as you know, was the breach or attack intentional or accidental?
DO NOT READ OUT
INTERVIEWER NOTE: IF INTENTIONAL BREACH/ATTACK, BUT ONLY SUCCEEDED BY ACCIDENT (E.G. LACK OF OVERSIGHT), CODE AS INTENTIONAL

Intentional
Accidental
(SINGLE CODE; ALLOW DK)

Q70.CONTING DELETED PRE-PILOT IN 2019 SURVEY

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q71.RESTORE
How long, if any time at all, did it take to restore business operations back to normal after the breach or attack was identified? Was it ...
PROBE FULLY

No time at all
Less than a day
Between a day and under a week
Between a week and under a month
One month or more
DO NOT READ OUT: Still not back to normal
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)
Q72.DEALA
How many days of staff time, if any, were needed to deal with the breach or attack? This might include any time spent by staff directly responding to it, as well as time spent dealing with any external contractors working on it.
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL FOR TOOK SOME TIME BUT LESS THAN A DAY

WRITE IN RANGE 0–300
(SOFT CHECK IF >99; ALLOW DK AND NULL)

ASK IF DON'T KNOW HOW MANY DAYS OF STAFF TIME TO DEAL WITH THE BREACH OR ATTACK (DEALA CODE DK)
Q73.DEALB
Was it approximately … ?
PROBE FULLY

Under 5 days
5–9 days
10–29 days
30–49 days
50–99 days
100 days or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

Q74. DELETED PRE-PILOT IN 2017 SURVEY

Q75. DELETED PRE-PILOT IN 2017 SURVEY

READ OUT IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK, AND INCURRED COSTS FROM BREACHES OR ATTACKS (DISRUPTA NOT DK AND COSTA NOT NULL)
I am now going to ask you about the approximate costs of this particular breach or attack. We want you to break these down as best as possible into the direct costs, the recovery costs and the long-term costs, which will be explained to you.
[IF USING MICROSITE (MICROSITE CODE 1): For these next questions, you can again look on the "During Interview" tab on the website for some helpful guidance.]

ASK IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK, AND INCURRED COSTS FROM BREACHES OR ATTACKS (DISRUPTA NOT DK AND COSTA NOT NULL)
Q75A.DAMAGEDIR

[IF COSTA NOT REF AND COSTB NOT DK: You said earlier that all the breaches or attacks you experienced in the last 12 months have cost your organisation {IF COSTA NOT DK: ANSWER AT COSTA / IF COSTA CODE DK: ANSWER AT COSTB} in total.] Approximately how much, if anything, do you think the **direct results** of this single most disruptive breach or attack have cost your organisation financially? [IF NOT USING MICROSITE (MICROSITE CODE 2): This includes any costs such as:

- staff not being able to work
- lost, damaged or stolen outputs, data, assets, trade secrets or intellectual property
- lost {revenue/income} if people could not access your services online.]

[IF USING MICROSITE (MICROSITE CODE 1): This includes the costs listed on the website under “direct results”.]
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL IF NO DIRECT RESULT COST INCURRED
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£30,000,000
IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2): (SOFT CHECK IF >£99,999; ALLOW DK AND REF)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£99,999; ALLOW DK AND REF)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999; ALLOW DK, NULL AND REF)

ASK IF DON’T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEDIR CODE DK)
Q75B.DAMAGEDIRB
Was it approximately ... ?
PROBE FULLY

IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2):
Less than £100
£100 to less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 or more
DO NOT READ OUT: Don’t know

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3):
Less than £100
£100 to less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 or more
DO NOT READ OUT: Don’t know

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]):
Less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK, AND INCURRED COSTS FROM BREACHES OR ATTACKS (DISRUPTA NOT DK AND COSTA NOT NULL)
Q75C.DAMAGEREC
[IF COSTA NOT REF AND COSTB NOT DK: You said earlier that all the breaches or attacks you experienced in the last 12 months have cost your organisation {IF COSTA NOT DK: ANSWER AT COSTA / IF COSTA CODE DK: ANSWER AT COSTB} in total.] Approximately how much, if anything, do you think **the recovery** from this single most disruptive breach or attack has cost your organisation financially? [IF NOT USING MICROSITE (MICROSITE CODE 2): This includes any costs such as:

- additional staff time to deal with the breach or attack, or to inform {customers or stakeholders/beneficiaries, donors or stakeholders}
- costs to repair equipment or infrastructure
- any other associated repair or recovery costs.]

[IF USING MICROSITE (MICROSITE CODE 1): This includes the costs listed on the website under "recovery".]
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL IF NO RECOVERY COST INCURRED
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£30,000,000
IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2): (SOFT CHECK IF >£99,999; ALLOW DK AND REF)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£99,999; ALLOW DK AND REF)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999; ALLOW DK, NULL AND REF)

ASK IF DON'T KNOW RECOVERY COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEREC CODE DK)
Q75D.DAMAGERECB
Was it approximately ... ?
PROBE FULLY

IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2):
Less than £100
£100 to less than £500
£500 to less than £1,000

£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 or more
DO NOT READ OUT: Don't know

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3):
Less than £100
£100 to less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 or more
DO NOT READ OUT: Don't know

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]):
Less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million or more
DO NOT READ OUT: Don't know
(SINGLE CODE)

ASK IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK, AND INCURRED COSTS FROM BREACHES OR ATTACKS (DISRUPTA NOT DK AND COSTA NOT NULL)
Q75E.DAMAGELON
[IF COSTA NOT REF AND COSTB NOT DK: You said earlier that all the breaches or attacks you experienced in the last 12 months have cost your organisation {IF COSTA NOT DK: ANSWER AT COSTA / IF COSTA CODE DK: ANSWER AT COSTB} in total.] Approximately how much, if anything, do you think the **long-term effects** from this single most disruptive breach or attack **will end up costing** your organisation financially? [IF NOT USING MICROSITE (MICROSITE CODE 2): This includes any costs such as:

- loss of share value
- loss of {investors/donors} or funding
- long-term loss of customers (including potential new customers or business)
- handling customer complaints or PR costs
- compensation, fines or legal costs.]

[IF USING MICROSITE (MICROSITE CODE 1): This includes the costs listed on the website under "long-term effects".]
PROBE FOR BEST ESTIMATE BEFORE CODING DK
CODE NULL IF NO LONG-TERM EFFECTS COST INCURRED

REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£30,000,000
IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2): (SOFT CHECK IF >£99,999; ALLOW DK AND REF)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£99,999; ALLOW DK AND REF)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999; ALLOW DK, NULL AND REF)

ASK IF DON'T KNOW LONG-TERM EFFECT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGELON CODE DK)
Q75F.DAMAGELONB
Was it approximately ... ?
PROBE FULLY

IF SMALL (SIZEA CODE<50 OR SIZEB CODES 1–2):
Less than £100
£100 to less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 or more
DO NOT READ OUT: Don't know

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3):
Less than £100
£100 to less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 or more
DO NOT READ OUT: Don't know

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]):
Less than £500
£500 to less than £1,000
£1,000 to less than £5,000
£5,000 to less than £10,000
£10,000 to less than £20,000
£20,000 to less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £1 million
£1 million to less than £5 million
£5 million or more
DO NOT READ OUT: Don't know

(SINGLE CODE)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q75G.BOARDREP

Were your organisation's [directors or senior management/trustees] made aware of this breach, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q76.REPORTA

Was this breach or attack reported to anyone outside your organisation, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK IF REPORTED (REPORTA CODE 1)

Q77.REPORTB

Who was this breach or attack reported to?
DO NOT READ OUT
PROBE FULLY (“ANYONE ELSE?”)

Action Fraud
Antivirus company
Bank, building society or credit card company
Centre for the Protection of National Infrastructure (CPNI)
CERT UK (the national computer emergency response team)
Cifas (the UK fraud prevention service)
Charity Commission
Clients/customers
Cyber Security Information Sharing Partnership (CISP)
Information Commissioner's Office (ICO)
Internet/Network Service Provider
National Cyber Security Centre (NCSC)
Outsourced cyber security provider
Police
Professional/trade/industry association
Regulator (e.g. Financial Conduct Authority)
Suppliers
Was publicly declared
Website administrator
Other government agency
Other *WRITE IN*
(MULTICODE; ALLOW DK)

Q77A.NOREPORT DELETED PRE-PILOT IN 2018 SURVEY

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–9] OR DISRUPTA NOT DK)

Q78.PREVENT

What, if anything, have you done since this breach or attack to prevent or protect your organisation from further breaches like this?

DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")
CODE NULL FOR "NOTHING DONE"

Additional staff training/communications
Additional vetting of staff or contractors
Changed nature of the business/activities carried out
Changed/updated firewall/system configurations
Changed which users have admin/access rights
Created/changed backup/contingency plans
Created/changed policies/procedures
Deployed new systems
Disciplinary action
Formal post-incident review
Increased monitoring of third parties' cyber security
Increased spending on cyber security
Installed/changed/updated antivirus/anti-malware software
Outsourced cyber security/hired an external provider
Penetration testing
Recruited new staff
Other *WRITE IN*
(MULTICODE; ALLOW DK AND NULL)

Q78B.NOACT DELETED POST-PILOT IN 2017 SURVEY

GDPR

SCRIPT TO ROTATE GDPRFINE AND GDPRREP

ASK ALL

Q78X.GDPRFINE

Before this interview, had you heard that organisations can be fined by the Information Commissioner's Office for cyber security breaches involving personal data?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK ALL

Q78Y.GDPRREP

Before this interview, had you heard that organisations need to report cyber security breaches involving personal data to the Information Commissioner's Office, within 72 hours of discovering them?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK ALL
Q78C.GDPRAWARE
A new data protection law called the General Data Protection Regulation, or GDPR, came into effect in May 2018. Before this interview, had you heard of the General Data Protection Regulation, or GDPR?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK ALL WHO ARE AWARE (GDPRAWARE CODE 1)
Q78D.GDPRCHANGE
Has your organisation made any changes or not to the way you operate in response to GDPR?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK ALL HAVE MADE CHANGES (GDPRCHANGE CODE 1)
Q78E.GDPRCYBER
Have any of these changes been related to your cyber security policies or processes, or not?

Yes
No
(SINGLE CODE; ALLOW DK)

ASK ALL HAVE MADE CHANGES (GDPRCYBER CODE 1)
Q78F.GDPRWHAT
What changes has your organisation made related to your cyber security policies or processes?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")

Additional staff training/communications
Additional vetting of staff or contractors
Changed nature of the business/activities carried out
Changed/updated firewall/system configurations
Changed which users have admin/access rights
Created/changed backup/contingency plans
Created/changed policies/procedures
Deployed new systems
Formal post-incident review
Increased monitoring of third parties' cyber security
Increased spending on cyber security
Installed/changed/updated antivirus/anti-malware software
Outsourced cyber security/hired an external provider
Penetration testing
Recruited new staff
Other *WRITE IN*

(MULTICODE; ALLOW DK)

Recontact and follow-up

ASK ALL
Q79.RECON
This survey is part of a wider programme of research. Would you be happy to take part in a more bespoke interview with Ipsos MORI in January or February 2019, to further explore some of the issues from this survey? This interview would be more of a conversation on the specific issues faced by your organisation. It would still be completely confidential.
ADD IF NECESSARY: the interviews would last no longer than 45 minutes and those taking part would be offered a £50 cheque or a donation to the charity of their choice.

Yes
No
(SINGLE CODE)

ASK ALL
Q80.REPORT
We can email you a copy of the findings, as well as a helpcard with links to Government guidance on cyber security. Would you like either or both of these? The summary of findings will be sent after this research is published in early 2019?

Yes – copy of the findings
Yes – Government helpcard
No
(MULTICODE CODES 1–2)

ASK IF WANT RECONTACT OR REPORT/HELPCARD (RECON CODE 1 OR REPORT CODES 1–2)
Q81.EMAIL
IF WANT RECONTACT (RECON CODE 1): Would you be happy to give us an email address to contact you directly, so we can invite you to the follow-up interview? This email will only be used for this research, and we won't keep it after the project is finished.
IF DON'T WANT RECONTACT (RECON CODE 2): Can I please take an email address for this?

WRITE IN EMAIL IN VALIDATED FORMAT
(ALLOW REF)

READ OUT TO ALL
Thank you for taking the time to participate in this study. Before you finish I need to inform you that you can access the privacy notice online at csbs.ipsos-mori.com. 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 D: Topic guide

Prompts and probes	**Timings and notes**
Introduction	**2–3 minutes**
• Introduce yourself and Ipsos MORI – independent research organisation (i.e. independent of Government) • Commissioned through the Government's National Cyber Security Programme, by the Department for Digital, Culture, Media & Sport (DCMS) • Explain the research: we are speaking with businesses and charities to learn more about how they approach cyber security • Confidentiality: all responses are confidential • Length: around 45 minutes to 55 minutes • Get permission to digitally record (and interview may be transcribed to help with our analysis) to help with notes and for anonymised quotes for report GDPR added consent (once recorder is on): • Ipsos MORI's legal basis for processing is your consent to take part in this research. • Your participation in this research is voluntary. • You can withdraw consent for data to be used at any point before, during or after the interview. Can I check you are happy to proceed?	*The welcome helps to orientate the participant and gets them prepared to take part in the interview.* *Outlines the "rules" of the interview (including those we are required to tell them about under MRS guidelines). This includes GDPR-related consent.* *Make this very brief – we have already spoken to these individuals in the quantitative survey, so they should understand the background*
Context	**2–3 minutes**
What's the main business/product/service of your organisation? Could you briefly describe your role? • Is your role broader than cyber security? • What team or department are you in? • Are you a specialist in this area? • Do you have other specialist staff or senior managers working in this area? Who is in charge of making decisions on cyber security (e.g. around spending, policies, staff or outsourced providers)? Just briefly for now, how do you think the topic of cyber security affects your organisation? What would you say are the top two or three risks you might face?	*This section provides context to follow up on later in the interview, in terms of who is in charge and what they see as the risks.* *Make this very brief.*
Cyber security culture and prioritisation	**5-7 minutes**

In the survey, you told us that cyber security was a [very high / fairly high / fairly low / very low] priority for your organisation's senior management. Can you tell us a bit more about that answer? • Why did you give that specific answer? • What does that answer mean in practice? What do your senior managers do on this topic? How have they engaged with it? What would it look like if cyber security was a <u>higher</u> priority for your organisation? • What do you think you would be doing differently? • What would it mean for senior managers? Wider staff? Shareholders or donors? • How much do you feel you know about what you should be doing/best practice? How close do you think your organisation is to what you <u>should</u> be doing/best practice? • Do you think your senior managers are paying it the right level of attention? • Has their engagement changed over time? What has driven this? • What about wider staff? Shareholders or donors? • How do senior management make decisions on investment in cyber security? Where does cyber security fit in compared to your other priorities? • What are the bigger strategic priorities for your organisation? • What makes these more of a priority than cyber security? Do you think cyber security will become more or less of a priority for your organisation over the next 12 months? What is going to make this change? What would it take to make cyber security a higher priority for your organisation?	*What drives engagement in cyber security?* *What does it mean in practice when organisations say cyber security is a high priority?*
GDPR	**5-7 minutes**
The General Data Protection Regulation, sometimes called GDPR, is a new law covering how organisations have to handle personal data. It came into force in May 2018. How do you think GDPR has impacted on cyber security in your organisation?	*Has GDPR made cyber security more of a priority since it came into force?* *Has this impact lasted, or was it just a temporary focus around when GDPR became law (in May 2018)?*

Has cyber security become any more of a priority since GDPR came into force? How has it impacted on: • the working culture/how staff treat cyber security • how much of a priority cyber security is to senior managers • how/how often senior managers get updated on cyber security • the actions you take to manage cyber risks • who you talk or report to if you have a cyber security breach • investment in cyber security? Has GDPR had any negative impacts on cyber security? • Has it narrowed the focus of senior managers? • Has it moved resources/spending away from other aspects? Do you think the effects of GDPR will last/continue? • Are you still making changes due to GDPR? What changes? • Do people in the organisation still talk about it? Senior managers? Wider staff? • Do you think it will still be an issue this time next year? Will staff/senior managers have forgotten about it?	*Alternatively, has GDPR crowded out cyber security in any way, by narrowing the focus to data protection?*
Risk management and the supply chain	**10 minutes**
What do you know about your suppliers' attitudes towards cyber security? • Have you been affected by a cyber security breach in your supply chain before? What happened? What have you done/ changed since then? • Have you considered your suppliers/subcontractors/supply chain as a source of cyber risk before? Is cyber security considered as a risk when you choose a supplier? How does it influence/factor into your choices? How do you monitor the cyber security of your suppliers? • How closely do you work with your suppliers in terms of cyber security? How often do you discuss it with them? • Is this a one-off exercise undertaken during procurement or is it an ongoing process with each supplier? Is it the same standard for all suppliers or different for each one? • What influence do you have over them? How do/could you influence their behaviour?	*Are suppliers seen as a risk?* *How do organisations manage risk in the supply chain?* *What kind of standards are organisations enforcing on suppliers and how adequate do they feel these are?* *Could these standards be improved or made easier to implement?*

• How much can you control this source of risk? What are you doing/should you be doing to manage this risk? Do you feel confident in your ability to monitor your supply chain's security? • What sorts of challenges do you face in monitoring and upholding your suppliers' cyber security? • Is there any kind of support or guidance which would help you to monitor your suppliers more effectively? Have you ever considered your wider supply chain, such as your suppliers' suppliers, as a source of cyber security risk before? • Do you know if your suppliers require their own suppliers to meet specific standards? How important would this be?	
Information sources and Government guidance	**10 minutes**
What kinds of things do you remember seeing or hearing in the news about cyber security? What impact have these stories had on your organisation? • Have they been discussed in the organisation? Did senior managers talk about them? • Have they led to any changes in approach? In staff attitudes? • Do you feel these stories have had any lasting impact? • Do these sorts of stories help you to know what to do on cyber security, or do they make it more confusing? If you were searching for guidance on cyber security, where would you look? • Who would you expect to give you guidance about cyber security? • Are there any sources you would trust more than others? • E.g. software/security firms, family/friends, professional contacts, outsourced providers, other businesses/charities, trade bodies, Government, Charity Commission etc.? Have you sought out any cyber security guidance from the Government? Can you tell me a bit about this? • What areas have you sought Government guidance on? • What prompted you to look for this? • What source of information did you use? • How much did you know about the guidance the Government provides? • Did you do anything as a result of this guidance?	*How aware are people of key messaging in Government sources of info? Has this changed over time? How salient is this in comparison to general news coverage and GDPR?*

• How helpful did you find the Government guidance? How clear is it? Did it meet your needs? How could it be improved? In your experience, how has Government guidance on cyber security changed over the last few years? Has it improved? Is it more useful now? How do these improvements make a difference to you?	

N.B. we will only ask up to one of these three coloured sections in an interview. The recruitment details will be colour-coded to show which sections, if any, are relevant, and which ones to prioritise. If there are multiple colours, prioritise the sections in the order they are here (i.e. insurance is the top priority).

SECTION ONLY RELEVANT IF FLAGGED BROWN IN THE SAMPLE (PRIORITY #1): Insurance	**7-8 minutes**
In the survey, you mentioned that you have a cyber security insurance policy. What was the motivation behind getting this? What do you think you gain from having cyber security insurance? What impact does having insurance have on your level of risk? How do you think having insurance has changed the organisation's approach to cyber security? • What would you be doing differently if you didn't have cyber security insurance? • Would you need to take any other preventative measures if you didn't have cyber insurance? • Has it made senior managers any more or less conscious of cyber security? What about wider staff? What other impact has it had?	*How has getting cyber security insurance affected attitudes to cyber risk?* *Is cyber security insurance seen as something that helps to deal with risks (although the risks are still there) or as something which just moves the risk to the insurance firm?*
SECTION ONLY RELEVANT IF FLAGGED BLUE IN THE SAMPLE (PRIORITY #2): Experience and cost of breaches	**7-8 minutes**
You mentioned in the survey that you have experienced a cyber security breach in the past year. Thinking about the most recent example, can you tell me briefly what happened? • How did you deal with the breach? • How well do you think your organisation dealt with the breach? What could have been improved? What did you learn from this? • Have there been any organisational or cultural changes as a result?	*How do organisations measure the cost and impact of breaches? Do they take indirect costs, and the cost to wider stakeholders into account? Has the breach prompted them to do anything differently?*

When thinking about the financial impact of the breach/breaches, what kinds of things would you be considering within this? • Have you measured/estimated the financial impact? How did you go about this? • How much have you thought about indirect costs, like lost productivity, lost business, or competitive edge (e.g. if intellectual property is stolen)? • How much have you thought about wider costs outside your business, e.g. to customers, shareholders or donors, or other stakeholders? • How much have you considered other indirect impacts like reputational damage? • How easy or hard is it to measure these things? How well would you say your organisation's senior managers understand the full cost of a cyber security breach? What aspects might they underestimate?	
SECTION ONLY RELEVANT IF FLAGGED GREEN IN THE SAMPLE (PRIORITY #3): Outsourced providers	**7-8 minutes**
You told us in the survey that you have an outsourced provider to manage your cyber security. I'd like to focus on this for a bit. What aspects of cyber security do you outsource? What services/functions/tools do they provide? What aspects do you still carry out in-house? • Why did you decide to outsource these aspects cyber security and not others? • How long have they worked with you? • Do you feel able to do the things in-house that they won't do for you? What other services/functions/tools would you want an external provider to provide? Why have you not requested these things? NOTE DOWN ANY SPECIFIC SERVICES/FUNCTIONS RAISED (ALREADY PROVIDED AND ONES THEY WANT TO BE PROVIDED), IN THE EXACT WAY THAT PARTICIPANTS DESCRIBE THEM. NOTE IF THEY USE ANY OF THE FOLLOWING TERMS: • information risk assessment and management • identification, authentication and access control • network security • end-user device security • monitoring, detection and analysis • incident response and management	*What kind of products and services provided by outsourced providers are organisations using or would they useful? Does having an outsourced provider mean that people feel less responsible for cyber security?* *We want to take note of the specific services/functions/tools/products that organisations are currently using and want to use. We have a list from DCMS, as they want to know if organisations are mentioning any of these terms and using the same kind of language as seen here.*

• supervisory control and data acquisition (SCADA) and information control systems • training, awareness and education • cyber professional services. Would your provider help you during a cyber security incident if it happened? • Why have/haven't you contracted them to do this? • Do you feel adequately prepared to deal with an incident in-house? How has the security culture changed with the outsourced provider in place? • Do you feel it has made your organisation more secure? • Are senior managers/wider staff any more or less security-conscious as a result? Do you feel having an outsourced provider has changed how you manage cyber risk and/or deal with breaches?	

N.B. the following sections are relevant for all interviews again.

SECTION ONLY RELEVANT IF FLAGGED PURPLE IN THE SAMPLE: Brief check on 2FA	**1 minute**
Just before we finish, we want to ask about a specific response you gave in the survey. You said that your organisation used two-factor authentication to access restricted files, or log into your own websites or apps. Can you very briefly tell me what kinds of things you were including in your answer?	*This is just soft-checking a specific response they gave in the survey. We want to know if they might have misinterpreted the question.*
Help card sent by email	**1 minute**
If you gave your consent for us to do so in the survey, we have sent you a help card by email. Do you remember receiving the help card? Was it useful? Did you find the information in it relevant to you? Is there any way it could have be improved upon?	*Check how useful the help card was, which was sent by email and how could it could have been improved upon.*
Wrap up	**2-3 minutes**
Overall, what do you think is the one thing I should take away from the discussion today? IF NOT ON PROFILE INFORMATION, COLLECT INCENTIVE DETAILS (£50 CHEQUE, BANK TRANSFER OR CHARITY DONATION) THANK AND CLOSE	*Wrap up interview.*

Appendix E: Further information

1. The Department for Digital, Culture, Media and Sport would like to thank the following people for their work in the development and carrying out of the survey and for their work compiling this report.

    - Kelly Finnerty, Ipsos MORI Social Research Institute
    - Helen Motha, Ipsos MORI Social Research Institute
    - Jayesh Navin Shah, Ipsos MORI Social Research Institute
    - Professor Mark Button, Institute for Criminal Justice Studies, University of Portsmouth
    - Dr Victoria Wang, Institute for Criminal Justice Studies, University of Portsmouth

2. The Cyber Security Breaches Survey was first published in 2016 as a research report, and became an Official Statistic in 2017. The previous reports can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey. This includes the full report, infographics and the technical and methodological information for each year. The next version of the Cyber Security Breaches Survey is expected to be published in 2020.

3. The responsible DCMS statistician for this release is Rishi Vaidya. For enquiries on this release, please contact Rishi on 0207 211 2320 or evidence@culture.gov.uk.

4. For general enquiries contact:

    Department for Digital, Culture, Media and Sport
    100 Parliament Street
    London
    SW1A 2BQ

    Telephone: 020 7211 6000

5. DCMS statisticians can be followed on Twitter via @DCMSInsight.

6. The Cyber Security Breaches Survey is an Official Statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https://www.statisticsauthority.gov.uk/code-of-practice/. Details of the pre-release access arrangements for this dataset have been published alongside this release.

4th Floor
100 Parliament Street
London
SW1A 2BQ