Department for Digital, Culture, Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

Cyber Security Breaches Survey 2018

Technical annex

This technical annex supplements a main statistical release by the Department for Digital, Culture, Media and Sport (DCMS). The main release covers findings from the Cyber Security Breaches Survey 2018. 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 2018 quantitative survey (from winter 2017) and qualitative survey (from early 2018), 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, for the first time in this 2018 release, charities. The quantitative survey was carried out in winter 2017 and the qualitative survey in early 2018. 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 Summary of methodology

There were two strands to the survey:

- A quantitative random probability telephone survey of 1,519 UK businesses and 569 UK registered charities was undertaken from 9 October 2017 to 14 December 2017.
- A qualitative survey consisting of 50 in-depth interviews were undertaken in January and February 2018 to follow up with businesses and charities that had participated in the survey, as well as higher education institutions.

1.2 Strengths and limitations of the 2018 survey

While there have been other surveys about cyber security in organisations in recent years, these have often used partially representative sampling or 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 UK registered charities in all income bands.

The 2018 survey shares the same strengths as the 2016 and 2017 surveys:

- 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 take into account 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. Two main limitations might be considered to be as follows:

- 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. 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).

- The qualitative in-depth interviews did not feature any examples of the kinds of substantive cyber security breaches that have featured in news and media coverage of the topic. It is therefore outside the scope of this survey to provide significant insights into how the largest UK businesses and charities deal with these especially substantive breaches, which may cost in the range of hundreds of thousands, or even millions of pounds.

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 and 2017 surveys. There were important changes in the scope of the survey in 2018, although these do not typically affect comparability:

- For the first time in this survey series, UK registered charities were included. Previous surveys only covered UK businesses. The quantitative survey findings for both groups have been reported separately, rather than as a merged sample of all UK organisations. This is because there is no population profile information for UK businesses and charities combined.
- The quantitative survey business sample has also been expanded to include mining and quarrying businesses (SIC sector B) for the first time. As of April 2018, this sector is estimated to account for under 0.1 per cent of all UK businesses, so the addition of this sector has not meaningfully impacted on the comparability of findings across years.
- A small number of questions from the 2016 and 2017 quantitative surveys were deleted in 2018 to make way for new questions. Section 2.1 summarises these changes. In the main report, comparisons to 2016 and 2017 findings are only made where valid (i.e. where questions were consistent).
- The qualitative survey specifically included three interviews with higher education institutions (including two universities). This was highlighted as an important subsector for DCMS and the National Cyber Security Centre. These interviews, as with the wider qualitative survey, are not intended to be representative but have given DCMS and its partners some specific insights about this subsector.

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

The questionnaire and all other survey instruments were developed by Ipsos MORI and the Institute for Criminal Justice Studies (ICJS), and approved by DCMS. Development for this year's survey took place over three stages from July to September 2017:

- stakeholder conversations (mainly by email) involving Government, three general business representative bodies, five trade associations, seven IT or security representative bodies, four large businesses, and two major charities
- cognitive testing interviews with four businesses and six charities
- a pilot survey, consisting of 20 interviews with businesses and 20 with charities.

Stakeholder research

The stakeholder research was intended to:

- clarify the key cyber security issues facing organisations, including any new issues arising since the 2017 survey
- review the 2017 questionnaire, survey instruments and findings, to assess gaps in knowledge and new question areas to be included in 2018
- help understand how to adapt the survey for charities, in terms of the language used in the questionnaire and the sampling approach.

There was less stakeholder research carried out by the Ipsos MORI team in this latest survey. This was because DCMS had already liaised with various Government stakeholders about the survey, and expected most questions to remain the same as before.

Interviews were carried out with representatives from the National Cyber Security Centre (NCSC) and two major charities, mainly to help inform the expansion of the survey to include charities for the first time. In addition, Ipsos MORI sent "keeping in touch" emails to all the business and cyber security stakeholder organisations that had taken part in the 2017 survey, giving them the opportunity to give feedback on that survey.

Following this stage, the 2017 questionnaire was amended with provisional new questions for testing, guided by DCMS. The reassurance email for respondents and pre-interview questions sheet (see Appendix A for a copy) were also updated.

The main changes to the questionnaire were as follows:

- Text substitutions were added to make the language and references appropriate for charities. For example, turnover was substituted for income, and references to directors or senior managers were adapted to also include trustees.
- New questions split organisations up into for-profit businesses, not-for-profit businesses and charities, and asked charities to identify their main charitable area.
- New attitudinal questions were added. These explored potential cyber skills shortages and gaps, and also a sense of information overload on cyber security.
- Questions on outsourced cyber security providers and cyber insurance were expanded. The questionnaire now breaks down whether organisations currently have an outsourced provider or intend to get one in the future. It also asks more specifically about whether organisations have cyber insurance, rather than more general business liability insurance. Finally, it splits out organisations that do not have insurance into those that have or have not considered it before.

Cognitive testing

The cognitive testing was intended to test comprehension of the new questions for 2018, as well as the appropriateness of the language used for charities. Interviews were carried out by the Ipsos MORI research team.

Participants were recruited by telephone by Ipsos MORI. The business sample was purchased from the Dun & Bradstreet business directory, while the charity sample comprised a random selection of charities from the charity regulator databases in each UK country. Recruitment quotas were applied and a £50 incentive was offered[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 at this stage were minor and highly question-specific. Some of the relatively more substantive changes were:

- changing the attitudinal questions around skills shortages and skills gaps, so that respondents were clearer on the difference between the two (skills shortages being about having enough *people* in the organisation dealing with cyber security, and skills gaps being about those in the organisation having enough *skills* to do their job effectively)
- adding questions on awareness of the General Data Protection Regulation (GDPR), and whether this had affected the organisation's approach to cyber security.

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).

Pilot fieldwork was undertaken by Ipsos MORI interviewers between 18 and 23 September 2017. Again, quotas were applied to ensure the pilot covered different-sized businesses from a range of sectors, and charities with difference incomes and from different countries. In total, 20 interviews were carried out with businesses and 20 with charities.

The pilot sample was taken from the same sample frames used for the main stage survey for businesses and charities (see next section). In total, 280 business leads and 352 charity leads were randomly selected.

Not all of these leads were used to complete the 40 pilot interviews. In the end, 127 untouched business leads and 192 charity leads from the pilot were released again for use in the main stage survey.

The main changes made following the pilot survey were cuts of around one minute, to bring the questionnaire length down to within c.22 minutes for the main stage.

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

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

2.2 Survey microsite

As in the 2017 survey, a publicly accessible microsite[2] 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 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 the main sample frame for Government surveys of businesses and for compiling official statistics.

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 2017, organisations in the agriculture, forestry and fishing sectors (SIC 2007 category A) were also excluded. Cyber security was judged to be a less relevant topic for these organisations, given their relative lack of e-commerce.

---

[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.

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 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 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 is set to improve for future surveys, as the database becomes more comprehensive.

Sample selection

In total, 53,783 businesses were selected from the IDBR. This is much higher than the 27,948 businesses selected for the 2017 survey. It reflects that the sample quality (in terms of telephone coverage and usable leads) was considerably lower than expected in 2017.

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, disproportionate sample targets were set for micro (1 to 9 staff), small (10 to 49 staff), medium (50 to 249 staff) and large (250 or more staff) businesses. DCMS also identified specific sector groupings for which they wanted to boost the sample. These were sector groupings that were assumed to have very different approaches to cyber security based on the 2016 and 2017 surveys, and based on anecdotal evidence: education; finance or insurance; health, social care or social work; information or communications; and manufacturing. 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)	3,592	266	445	4,303
F	Construction	5,056	190	182	5,428
G	Retail or wholesale (including vehicle sales and repairs)	4,105	274	726	5,105
H	Transport or storage	4,238	122	244	4,604
I	Food or hospitality	2,698	168	121	2,987
J	Information or communications	7,405	170	286	7,861
K	Finance or insurance	644	222	355	1,221
L, N	Administration or real estate	7,770	173	476	8,419
M	Professional, scientific or technical	5,888	163	305	6,356
P	Education	2,057	126	119	2,302
Q	Health, social care or social work	2,131	177	124	2,432
R, S	Entertainment, service or membership organisations	2,558	72	135	2,765
	Total	**48,142**	**2,123**	**3,518**	**53,783**

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, 45,541 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. Telephone tracing was carried out (matching to both 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. Businesses that had

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

also been sampled for the Commercial Victimisation Survey 2018 (a separate Home Office survey with UK businesses taking place at the same time) were also removed to avoid contacting the same organisations for both surveys.

Following telephone tracing and cleaning, the usable business sample amounted to 12,697 leads (including the leads taken forward from the pilot). For the Scotland charities sample, 2,458 leads had telephone numbers after matching.

Table 2.2 breaks the business leads down by size and sector.

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)	1,044	238	348	1,630
F	Construction	821	175	174	1,170
G	Retail or wholesale (including vehicle sales and repairs)	1,310	243	526	2,079
H	Transport or storage	542	105	218	865
I	Food or hospitality	707	133	108	948
J	Information or communications	488	140	245	873
K	Finance or insurance	364	190	311	865
L, N	Administration or real estate	862	148	420	1,430
M	Professional, scientific or technical	622	132	248	1,002
P	Education	277	108	110	495
Q	Health, social care or social work	291	156	113	560
R, S	Entertainment, service or membership organisations	602	59	119	780
	Total	**7,930**	**1,827**	**2,940**	**12,697**

The usable leads for the main stage survey were randomly allocated into separate batches for businesses and charities. The first business batch included 4,650 leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band from the 2017 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 1,000 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

Main stage fieldwork was carried out from 9 October 2017 to 14 December 2017 using a Computer-Assisted Telephone Interviewing (CATI) script. This was a similar overall fieldwork period as for the 2017 survey.

In total, 1,519 interviews were completed with businesses, and 569 with charities. The average interview length c.22 minutes (in line with 2017).

Fieldwork preparation

Prior to fieldwork, telephone interviewers were briefed by the Ipsos MORI research team. 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

Random-probability sampling was adopted 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 all but six cases), leads were actually called 12 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.

Several steps were taken 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 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) and the Association of British Insurers (ABI), 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.

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

Fieldwork outcomes and response rates were monitored 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 calculation for businesses.[6] Table 2.4 shows the equivalent outcomes and response rate for charities.

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 calculation for businesses

Outcome	Total
Total sample loaded	9,768
Completed interviews	1,519
Incomplete interviews	114
Ineligible leads – established during screener[7]	164
Ineligible leads – established pre-screener	277

[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.

Outcome	Total
Refusals	2,191
Unusable leads with working numbers[8]	833
Unusable numbers[9]	1,086
Working numbers with unknown eligibility[10]	3,584
Expected eligibility of screened respondents[11]	91%
Expected eligibility of working numbers[12]	71%
Unadjusted response rate	16%
Adjusted response rate	25%

Table 2.4: Fieldwork outcomes and response rate calculation for charities

Outcome	Total
Total sample loaded	2,309
Completed interviews	569
Incomplete interviews	32
Ineligible leads – established during screener	12
Ineligible leads – established pre-screener	86
Refusals	346
Unusable leads with working numbers	202
Unusable numbers	186
Working numbers with unknown eligibility	876
Expected eligibility of screened respondents	98%
Expected eligibility of working numbers	75%
Unadjusted response rate	25%
Adjusted response rate	36%

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

The adjusted response rate for businesses in the 2018 survey was moderately lower than for 2017 (27%). The reasons for this are unclear, but the low response rates overall across businesses and charities reflect 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. Several steps have been taken each year to reduce these barriers to taking part, including reassurances around confidentiality and setting up the survey microsite.

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 ultimately no post-fieldwork editing was needed to remove outliers.

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 the existing code frame. It was also possible for new codes to be added where enough respondents – 10 per cent or more – had given a similar answer outside of the existing code frame. The accuracy of the coding was verified by the Ipsos MORI project team, who checked and approved each new code proposed.

SIC coding was not undertaken and 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

Rim weighting (random iterative method weighting) was applied 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 businesses 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 2017 and 2016 surveys, non-interlocking rim weighting by size and sector was undertaken for businesses. Weighting by region was not applied to the business sample but it should be noted that the final weighted data are closely aligned with the population region profile. Interlocking weighting was also possible, but would have potentially resulted in very large weights – this would have reduced the statistical power of the survey results without making any considerable difference to the weighted percentage scores at each question.

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

Table 2.5 and Table 2.6 shows the unweighted and weighted profiles of the final data.

Table 2.5: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Micro or small (2–49 staff)	66%	97%
Medium (49–249 staff)	17%	3%
Large (250+ staff)	17%	1%
Sector		
Administration or real estate	10%	12%
Construction	10%	12%
Education, health or social care	6%	6%
Entertainment, service or membership organisations	7%	7%
Finance or insurance	7%	2%
Food or hospitality	8%	10%
Information, communication or utilities	7%	6%
Manufacturing	9%	7%
Professional, scientific or technical	9%	15%
Retail or wholesale	14%	18%
Transport or storage	6%	3%
Region		
East Midlands	6%	6%
Eastern	11%	13%
London	15%	13%
North East	2%	2%
North West	9%	8%
Northern Ireland	4%	5%
Scotland	8%	8%
South East	17%	16%
South West	9%	10%
Wales	4%	4%
West Midlands	8%	8%
Yorkshire and Humberside	7%	7%

Table 2.6: Unweighted and weighted sample profiles for charity interviews

	Unweighted %	Weighted %
Size		
£0 to under £10,000	15%	42%
£10,000 to under £100,000	21%	36%
£100,000 to under £500,000	24%	14%
£500,000 to under £5 million	22%	6%
£5 million or more	14%	2%
Country		
England and Wales	80%	85%
Scotland	15%	12%
Northern Ireland	5%	3%

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 was agreed with DCMS that for those who gave banded responses, a numeric response would be imputed – as it was in the 2017 and 2016 analysis. 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 2017 survey dataset.

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
- two merged sector variables (sector_comb1 and sector_comb2)
  - one matches the sector groupings used in the 2017 survey report, for direct comparison purposes only
  - one matches the more granular sector groupings used in the 2018 report
- 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).

In addition, this dataset has two variables covering use of outsourced cyber security providers: outsource (Q9) and manage2 (Q29). These reflect that this question was asked at two different points in the questionnaire, in slightly different ways. For reporting purposes, outsource has been used. However, manage2 was also kept in for historic reasons, and to keep the routing into the subsequent nopol (Q29B) question unchanged.

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.[13] 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 data tables.

[13] 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

The sample for the majority of the 50 in-depth interviews was taken from the quantitative survey. Respondents were asked in 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, 691 businesses (45%) and 300 charities (53%) agreed to be recontacted. Ultimately, 27 interviews were undertaken with businesses and 20 were with charities.

In the 2018 survey, DCMS also specifically wanted qualitative insights on cyber security in higher education institutions. The business survey recontact sample did not include many leads fitting this category, but one further and higher education college was recruited from this sample. To make up the remaining interviews, a further two universities were recruited from the Ipsos MORI recruiters' networks.

3.2 Recruitment and quotas

Recruitment for the qualitative survey was carried out by telephone. A £50 incentive was offered[14] to encourage participation.

Soft recruitment quotas were used 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
- organisations where directors or trustees see cyber security as a very high priority, or very low priority
- organisations that have cyber insurance or that have considered getting it
- organisations that outsource or intend to outsource their cyber security.

3.3 Fieldwork

All telephone fieldwork was undertaken by the Ipsos MORI research team in January and February 2018. Interviews lasted around 45 minutes on average.

The interview topic guide was drafted by Ipsos MORI and was approved by DCMS. It was developed taking into consideration the quantitative findings, and where it would be beneficial to understand the factors and reasons behind these findings. The topic guide covered the following areas:

- what organisations thought "good" cyber security looks like and how they knew or observed if they were doing a good enough job on this
- what information, advice or guidance they wanted on cyber security, and what they thought was missing
- the perceptions of cyber security insurance, and what informed the decision to take out a cyber insurance policy
- how organisations go about choosing outsourced cyber security providers
- what motivates or would motivate organisations' directors or trustees to change their behaviour on cyber security, or make it more of a business priority.

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

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

Tables 3.1 and 3.2 shows a profile of the 27 interviewed businesses by size and sector.

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

SIC 2007 letter	Sector description	Total
B, C, D, E	Utilities or production (including manufacturing)	3
F	Construction	2
G	Retail or wholesale (including vehicle sales and repairs)	2
H	Transport or storage	2
I	Food or hospitality	1
J	Information or communications	1
K	Finance or insurance	3
L, N	Administration or real estate	1
M	Professional, scientific or technical	6
P	Education (excluding further or higher education institutions)	1
Q	Health, social care or social work	4
R, S	Entertainment, service or membership organisations	1
	Total	**27**

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

Size band	Total
Micro or small (1–49 staff)	13
Medium (49–249 staff)	8
Large (250+ staff)	6

Table 3.3 shows a profile of the 20 interviewed charities by income band. In one case, charity income was not on the sample and the charity could not provide it in the survey.

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

Income band	Total
£0 to under £10,000	2
£10,000 to under £100,000	4
£100,000 to under £500,000	4
£500,000 to under £5 million	4
£5 million or more	5
Unknown	1

3.4 Analysis

Interviews were summarised in a notes template. Throughout fieldwork, the core research team discussed interim findings and outlined areas to focus on in subsequent interviews. At the end of fieldwork, a final face-to-face analysis meeting was held, attended by DCMS, where key themes were drawn out.

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
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 (p39), Q46 (p40)	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 (p39)	This refers to how files are classified (e.g. public, internal use, confidential etc).
Document Management System	Q32 (p39)	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 (p40)	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) (p35)	Government Communications Headquarters – one of the main government intelligence services
GDPR	Q78C (p56), Q78D (p56)	The General Data Protection Regulation is a legal framework that sets guidelines for collection and processing of individuals within the European Union (EU).
IISP	Q24 (DO NOT PROMPT) (p35)	Institute of Information Security Professionals – a security body
Hacking	Q53A (p41), Q64A (p46), Q68 (DO NOT PROMPT) (p48)	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) (p33), Q56A (p43), Q75A (p50)	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) (p35)	Information Security Forum – a security body
Malware	Q31 (p38), Q53A (p41), Q64A (p46), Q65 (p46), Q68 (DO NOT PROMPT) (p48), Q78 (DO NOT PROMPT) (p55), Q78F (p56)	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).
Outsourced provider	Q9C (p27), Q29 (p37)	Outsourced organisations that deal with an organisation's cyber security as part of a wider IT support role
Penetration testing	Q22 (p55), Q52 (p56), Q78 (DO NOT PROMPT) (p55), Q78F (p56)	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 (p26), Q32 (p39), Q67 (p47)	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 (p41), Q64A (p46)	Malicious software that blocks access to a computer system until a sum of money is paid
Removable devices	Q32 (p39)	Removable devices are portable things that can store data, such as USB sticks, CDs, DVDs etc.
Restricting IT admin and access rights	Q31 (p38)	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.
Segregated guest wireless networks	Q31 (p38)	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 (p38)	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.

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

ASK ALL
S1.
Is this the head office for [SAMPLE CONAME]?

Yes
No – another organisation
No – not the head office ASK TO BE TRANSFERRED AND RESTART
No – any other reason CODE OUTCOME, THANK AND CLOSE *(CLOSE SURVEY)*
(SINGLE CODE)

READ OUT IF HEAD OFFICE (S1 CODE 1)
Hello, my name is … from Ipsos MORI, the independent research organisation. We are conducting an official survey on behalf of the UK Government's National Cyber Security Programme about how UK businesses, charities and other non-profit organisations approach cyber security. The purpose of this survey is not to sell any software or services – it is conducted annually to generate Government statistics.

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

ADD IF NECESSARY: the survey has been commissioned by the Department for Digital, Culture, Media and Sport as part of the UK Government's National Cyber Security Programme.

ADD IF NECESSARY: The survey will help the Government to understand what businesses, charities and other non-profit organisations currently do to prevent and deal with cyber security breaches or attacks, how important they think the issue is, and how any breaches or attacks have affected their organisation, including financially. The findings will inform Government policy and the guidance offered to businesses and other organisations.

IF UNSURE WHAT CYBER SECURITY IS: By cyber security, 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.

IF UNSURE WHO RELEVANT PERSON IS OR IF OUTSOURCE CYBER SECURITY: If there is no one who deals specifically with cyber security within your organisation, we would like to talk to the most senior person who deals with any IT issues. We know this may be the business owner, a trustee, Chief Executive, or someone else from the senior management team.

Would you be happy to take part in an interview around your organisation's approach to cyber security?

REASSURANCES IF NECESSARY

- Taking part is totally confidential and anonymous for all individuals and organisations.
- It doesn't matter if you have not had any cyber security or IT issues, or if you outsource your cyber security – we need to talk to a wide range of organisations in this survey and you will not be asked irrelevant questions.
- The survey is not technical and you don't need any specific IT knowledge to take part.
- We can share some of the questions with you by email, to help you find the right person to take part.
- Findings from the survey will be published on the GOV.UK website in early 2018, in order to help businesses like yours.
- Details of the survey are on the gov.uk website (https://www.gov.uk/government/publications/cyber-security-breaches-survey) and the Ipsos MORI website (csbs.ipsos-mori.com).
- If you prefer, rather than clicking on a link you can type "2017 SURVEY Ipsos MORI" into Google. You can see details of the survey by following the Ipsos MORI links or the GOV.UK links.
- 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.

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

- 170 refused – outsources cyber security
- 171 – soft refusal
- 172 refused – no cyber security issues/problems
- 173 refused – think survey is not genuine
- 174 refused – company no-name policy
- 175 refused – cyber security is commercially confidential
- 180 – wrong direct line
- 181 – duplicate business
- 182 – company accountant refusing
- 203 ineligible – sole trader at SIZEA
- 247 ineligible – no computer, website or online use
- 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 for [businesses/charities and other non-profit organisations]. The website gives examples of the kinds of questions we ask. I strongly recommend looking at this website before taking part. Other participants have told us it is helpful to see the main questions in advance, so they can talk to relevant colleagues and get the answers ready before the interview.

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 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)

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)

SCRIPT TO BASE BUSINESS/CHARITY TEXT SUBSTITUTIONS ON TYPEX (BUSINESS IF TYPEX CODES 1–2, ELSE CHARITY)

ASK ALL

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 £1,000
£1,000 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 £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)

Q5C.YEARSDELETED POST-PILOT in 2018 SURVEY

ASK IF CHARITY (SAMPLE TYPE=2)
Q5D.CHARITYO
Which one of the following best describes the main area that your charity works in?
READ OUT
INTERVIEWER NOTE: IF THEIR ACTIVITIES COVER MORE THAN ONE AREA, PROBE WHAT BEST DESCRIBES THE MAJORITY OF THEIR ACTIVITIES OR THEIR BIGGEST CURRENT ACTIVITY

Animals, conservation or environmental causes
Arts, culture or heritage
Economic, social or community development within the UK
Education or employment
Healthcare, social care, disability or ageing
Housing, homelessness or welfare
Human rights, equality or diversity
Overseas aid or development
Religious activities
Sport or recreation

Other WRITE IN
DO NOT READ OUT: Don't know
(SINGLE CODE)

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)

ASK IF ANY ONLINE SERVICES (ONLINE CODES 1–8)
Q7.CORE
To what extent, if at all, are online services a core part of the [goods or/charitable] services your organisation provides? Is it ...
READ OUT

To a large extent
To some extent
Not at all
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST CODE)

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
(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.HIGHDELETED POST-PILOT IN 2017 SURVEY

Q9B.RELPRIORITYDELETED POST-PILOT IN 2018 SURVEY

ASK ALL
Q9C.OUTSOURCE
Which of the following best represents your organisation when it comes to outsourcing cyber security? This can include outsourced organisations 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.LOWDELETED PRE-PILOT IN 2018 SURVEY

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

a. **DELETED PRE-PILOT IN 2018 SURVEY**
b. **DELETED PRE-PILOT IN 2018 SURVEY**
c. **DELETED PRE-PILOT IN 2018 SURVEY**
d. **DELETED PRE-PILOT IN 2018 SURVEY**
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 secure website to help you answer some of the questions and make the survey quicker. The link is csbs.ipsos-mori.com/during-interview. If you have a computer or phone, would you be happy to go to this website now, and have it open for the rest of the survey?
ADD IF NECESSARY: We can finish the survey without it, but we have heard from other businesses that having it open makes it easier for them.

Yes
No

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 (SALESA NOT REF OR SALESB CODES 1–7): 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)

Q16A.DELETED PRE-PILOT 2017 SURVEY

Q16B.DELETED PRE-PILOT 2017 SURVEY

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.EVALDELETED PRE-PILOT IN 2018 SURVEY

Q23.INSUREDELETED 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.COVERAGEDELETED 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
(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?")

Advised against it
Available policies are confusing
Available policies have restrictive conditions
Available policies not right for our organisation generally
Aware but have not prioritised it/weighed it up
Don't consider ourselves at risk/low risk
Existing measures good enough
Not affordable/costs too much/high premiums
Covered by another/general insurance policy
Cyber attack would not impact us much
Intend to get it/still looking
Market too new/undeveloped
Not aware of it/thought about it before
Offers insufficient coverage
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
Government – other *WRITE IN*
National Cyber Security Centre (NCSC)
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.FINDINFDELETED 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
(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.TRAINUSEDELETED 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.DELIVERDELETED POST-PILOT IN 2018 SURVEY

Q28.COVERDELETED 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
Encrypting personal data
Security controls on company-owned devices (e.g. laptops)
Only allowing access via company-owned devices
A segregated guest wireless network
Guidance on acceptably strong passwords
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.FOLLOWDELETED POST-PILOT IN 2017 SURVEY

ASK ALL
Q33.DOC
Are cyber security risks for your organisation documented in any of the following, or not?
READ OUT

In Directorate or Departmental risk registers
In a Company or Enterprise-level risk register
ONLY SHOW IF IDENT CODE 1: In an Internal Audit Plan
ONLY SHOW IF MANAGE CODE 4: In the Business Continuity Plan
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES)

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 5)
Q36.10STEPS
Are you aware of the government's 10 Steps to Cyber Security guidance, or not?

Yes
No
(DP AUTO-CODE 1 IF INFO CODE 6; ALLOW DK)

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

Yes
No
(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
(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
(ALLOW DK)

Q47.DELETED POST-PILOT IN 2016 SURVEY

Q48.CRITICALDELETED POST-PILOT IN 2017 SURVEY

Q49.COMMERDELETED PRE-PILOT IN 2018 SURVEY

Q50.PERSONDELETED PRE-PILOT IN 2018 SURVEY

Q51.VALIDADELETED POST-PILOT IN 2017 SURVEY

Q52.VALIDBDELETED 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.MONITORDELETED 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 >£9,999,999; 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
(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)

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)

Q70.CONTING

Was there a contingency plan in place to deal with this type of breach or attack, or not?
IF YES: Was this effective, or not?
DO NOT READ OUT

Yes, and it was effective
Yes, but not effective
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)

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 [customers/donors] 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 >£999,999; ALLOW DK AND REF)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£9,999,999; 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 >£999,999; ALLOW DK AND REF)

IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£9,999,999; 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 >£999,999; ALLOW DK AND REF)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£9,999,999; 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
(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
(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)
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.NOREPORTDELETED 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.NOACTDELETED POST-PILOT IN 2017 SURVEY

GDPR

ASK ALL

Q78C.GDPRAWARE

A new data protection law called the General Data Protection Regulation, or GDPR, will come into effect on 25 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 have your 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)

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 totally confidential and anonymous, and no identifying information will be passed onto the Government or anyone else • Length: around 45 minutes • Get permission to digitally record (and interview may be transcribed to help with our analysis)	*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).* *Make this very brief.*
Context	**2–3 minutes**
What's the main business/product/service of your organisation? How do you think the topic of cyber security affects your organisation? What are the main risks you face? Could you briefly describe your role? Is your role broader than cyber security? Who is in charge of making decisions (e.g. around spending on cyber security, policies, staff or outsourced providers)?	*This section provides context to follow up on later in the interview, in terms of who is in charge of the issue and what they see as the risks.* *Make this very brief.*
Risk and incident management, and culture	**10 minutes**
What does good cyber security look like for an organisation like yours? • What sorts of things should you be doing to manage risks? What sorts of things do/should you have in place? • What sorts of things should your board/trustees/staff/volunteers/students be doing? • How did you come to this view? Where have you seen/heard/been told this? • What could you improve upon? What might be missing? How do you know if you're well protected from the risks?	*What do organisations think "good" cyber security looks like? How do they know/observe/measure if they're doing a good enough job on this or not?* *How can you instil a security-conscious culture within organisations? In different sectors or types of organisations, maybe this culture comes from a different place (e.g. maybe investors*

- How do you observe/measure it? Any incident logging? Specific metrics? Risk assessments? Feedback from staff?
- If not measuring, how do you know if you're protected? What information/feedback are you getting? What/who are you relying on?

Describe the culture of your organisation when it comes to cyber security?

- How seriously would directors/trustees/staff/volunteers/ students treat the issue? How security-conscious are they? How much time do they spend on it?
- How/when is it considered? In day-to-day work/study (any examples)? Only when problems arise/something goes wrong?
- Where does this culture come from? An individual/individuals at the top? Usual practice across the sector? Following best practice? Regulation?
- Do investors/shareholders/donors/students ever raise the issue?
- Has the culture always been like this? How has it changed? Any changes after previous incidents/events/news stories?

How important/useful are the following? What makes the most difference? Which of these do you have/need? Why don't you have/need them? What would help you set them up?

- Written cyber security policies
- Incident management plans
- Education/training/the right skills
- Having specific directors or trustees in charge of/responsible for/taking an interest in cyber security
- Having a good cyber security provider (outsourced provider)

What difference has awareness raising/training made?

- How has this been carried out? Emails, meetings, webinars, internal vs. external training etc? What makes this the preferred way of doing things?
- What has worked well/less well in terms of raising awareness/delivering training? What might be improved?
- How easy has it been to find good training content/trainers?

have more clout in certain organisations).

Are they resigned to being breached/certain things being out of their control?

Why don't some organisations have policies or good processes in place? What information or guidance do they want/need to help set these things up?

Has any training provided to staff/volunteers/students met their needs, or not? What can make training more effective, or make better training easier to find?

Are organisations isolating action on cyber security to within their own organisation and missing out their suppliers as a source of risk? Could they change this?

Are cyber security breaches inevitable? How so? What kinds of risks are out of your control? Have you considered your suppliers/subcontractors/supply chains as a source of risk before? • What is the culture of your suppliers on this issue? How much of a risk do they pose to you? • What influence do you have over them? How do/could you influence their behaviour? • How much can you control this source of risk? What are you doing/should you do?	
Seeking information	**10 minutes**
What sorts of information or advice is missing or hard to find for an organisation like yours? What would be helpful? • Specific content? • Format, e.g. checklists? • Advice tailored to your size/sector? • Jargon-free? Any examples of jargon? Who would you expect to give you information, advice or guidance about cyber security? • E.g. software/security firms, outsourced providers, other businesses/charities, Government, Charity Commission etc? How do you keep up to date with the latest/biggest threats facing your organisation? • If you had to search for this information, how would you go about it? Where would you look? What search terms? • Would you go to Government/non-Government sources? What makes these more appealing? How clear is the information and advice out there? In our survey, many organisations told us they are not sure how they should act on the advice they have seen or heard around cyber security – in your view, what makes them say this? In our survey, many organisations said they had received and followed information or advice from their IT contractors or outsourced providers. In your case/view, how reliable/trustworthy would this advice be? What do you base that on?	*How do organisations get their information and advice on this topic?* *DCMS says organisations predominantly go to the private sector for information and advice on threats. Why might this be, rather than seeking and using Government advice?* *How can information and advice be improved or better-channelled to organisations?*

In our survey, very few organisations had sought out cyber security advice or guidance from the Government. In your view, why do you think that might be?	
SECTION ONLY RELEVANT IF FLAGGED GREEN IN THE SAMPLE: Insurance	**10 minutes**
In the survey, you mentioned that you have or considered getting a cyber security insurance policy. I'd like to focus on this for a bit. Can you describe the how you arrived at this decision? Interviewer note timeline of events. • What prompted thinking about this? Raised internally, or by an insurer/broker? After a breach? • What conversations did you have internally? What questions did directors/trustees have? • What conversations did you have with insurers? What questions did you ask them? What did they ask from you? What did you think of their demands? • What factors drove the final decision? What might make you change your mind in the future? What are your overall perceptions of cyber security insurance? • Of the products/market/insurers? • Is this from direct experience, or from what you have heard elsewhere? Probe for specific examples. What is your general perception of cyber security insurance policy providers and brokers?	*What prompted discussions about cyber security insurance within the organisation? How much of a role did the insurer play?* *What kinds of things did the insurer/broker raise/focus on? How was the discussion framed? Were they discussing the needs of the organisation purely from a cyber perspective, or in more general terms?*
SECTION ONLY RELEVANT IF FLAGGED BROWN IN THE SAMPLE: Outsourced providers	**10 minutes**
You told us in the survey that you have or intend to get an outsourced provider to manage your cyber security. I'd like to focus on this for a bit. What specific services do/would they cover? How long have they worked with you? Can you talk me through the decision to outsource your cyber security? • What prompted thinking about this? E.g. lacking skills within the organisation to manage cyber security? Typical to organisation's business model? After a breach?	*First question is just for context. We don't really mind what services are provided.* *Adapt probes as relevant in this section depending on whether they have a provider or are intending to get one in place.* *How much were organisations really considering the security offer of the provider relative to other providers – can they tell a good provider from a bad one?*

• What conversations did you have internally? What questions did directors/trustees have? How did you choose/do you intend to choose a specific provider? • What information did you need to make a decision? • If you were interviewing for a new provider right now, what would the process be? What questions would you ask them? How would you assess them? • Did you ask your current provider these questions? Why? What factors drove/will drive the final decision? • Did/does size/location matter, e.g. small local company versus large well-known provider (e.g. Microsoft)? • Did/does use of/access to cloud computing matter? What made this important? How do you judge whether one provider offers better security than another? • How easy is it to do this? • Do you feel you have the right information/guidance/skills to do this? What kinds of guidance, education or training might help/make it easier? How has the security culture changed with the outsourced provider in place? Are people more/less security-conscious now? What other changes have been made?	*What kinds of skills/guidance/training might the need/want to help with this?* *Does outsourcing encourage a more relaxed attitude to cyber security within the organisation/devolving of responsibility?*
Motivation and changing behaviour	**10 minutes (but if previous coloured sections not asked, then spend extra time here)**
Where does cyber security fit in compared to your other business priorities? What are the bigger strategic priorities for your business? What makes these more of a priority than cyber security? Now I'd like to talk a bit about what your organisation might do in the future. This time next year, how big an issue is cyber security likely to be for your organisation? What makes you say this? • Think risks are low for their type of organisation? Based on size, sector, business model etc? Have they assessed the risks?	*The intro to this section tries to establish whether/why this is an organisation that thinks cyber security doesn't really concern them, now or in the future (e.g. the archetypal construction firm that thinks, "we don't use IT, so it's not an issue"). In practice, you may have got a sense of this much earlier in the interview – possibly when discussing risks and culture –*

• How aware do they feel about the issue? Something they have ever considered before? • Just follow recommendations of outsourced providers? What more might you do to improve your organisation's cyber security? What kinds of things might stop your organisation from making these improvements/taking action? What is in the way? • Awareness/education/skills? Of whom (directors/trustees, staff, volunteers, investors/shareholders/donors) etc? • Costs too much? What would help overcome these barriers? • New policies/processes? • What kinds of information, advice or guidance? • Best ways to raise staff/volunteer/student awareness? • What kind of training? Format, content? Aimed at who? What difference would this make? Has this worked well in the past? Any good examples? • What has stopped you from doing these things so far? What more would you do if you had more money/funding for cyber security? What stops you from justifying this spend at the moment? What kinds of messages/arguments about the impact of cyber security would make most difference to an organisation like yours? To directors/trustees? Which of the following areas is most important for you to understand/would do most to convince organisations like yours? • How it impacts productivity/stops staff from carrying out day to day work • How it can lead to loss of revenue/share value/income • Repair/recovery costs • Potential fines from regulators/authorities/legal costs • Reputational damage (what does this mean to you?) • Preventing you from reaching customers/supplying goods or services • Complaints from customers • Complaints from investors/shareholders/donors/students	*so can move on to the later probes.* *Whose attitudes specifically might be holding back the organisation in making changes? Is it the directors/trustees, staff/volunteers, or investors/shareholders/donors etc?* *What arguments does Government need to make to overcome these barriers? And what arguments do people within the organisation need to make to change the culture? What kinds of messages would have the most impact/be the most important?* *If they say it costs too much, we want to challenge this – what would be needed to justify spending more? What would it have to affect?*

Wrap up	**2 minutes**
Is there anything that we haven't discussed that you would like to raise? Overall, what do you think is the one thing I should take away from the discussion today? Reassure about confidentiality. 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
    - Yasmin White, 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 next update to these statistics is expected to be the results of the next Cyber Security Breaches Survey. This iteration of the survey is expected to be carried out between autumn 2018 and winter 2018-19, with the results then being published later in 2019.

3. The Cyber Security Breaches Survey was first published in 2016 as a research report, and became an Official Statistic in 2017. The 2017 full report can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey. The 2017 statistical release includes the full report, infographics and the technical and methodological information.

4. 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.

5. For general enquiries contact:

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

    Telephone: 020 7211 6000

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

7. 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.

Department for Digital, Culture, Media & Sport

4th Floor
100 Parliament Street
London
SW1A 2BQ