Department for Culture Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

April 2017

Cyber Security Breaches Survey 2017

Annex

Dr Rebecca Klahr, Jayesh Navin Shah, Paul Sheriffs, Tom Rossington and Gemma Pestell
Ipsos MORI Social Research Institute

Professor Mark Button and Dr Victoria Wang
Institute for Criminal Justice Studies, University of Portsmouth

Contents

1 Overview 1
1.1 Summary of methodology 1
1.2 Strengths and limitations of the 2017 survey 1
1.3 Comparability to the Cyber Security Breaches Survey 2016 2
1.4 Comparability to the earlier Information Security Breaches Surveys 2
2 Survey approach technical details 3
2.1 Survey and questionnaire development 3
2.2 Survey microsite 5
2.3 Sampling 5
2.4 Fieldwork 8
2.5 Fieldwork outcomes and response rate 11
2.6 Data processing and weighting 12
3 Qualitative approach technical details 16
3.1 Sampling 16
3.2 Recruitment and quotas 16
3.3 Fieldwork 16
3.4 Analysis 17
Appendix A: pre-interview questions sheet 18
Appendix B: interviewer glossary 19
Appendix C: questionnaire 21
Appendix D: quailtative topic guide 52

List of Tables

Table 2.1: Pre-cleaning selected sample by size and sector 6
Table 2.2: Post-cleaning available sample by size and sector (excluding leads used in the pilot) 7
Table 2.3: Fieldwork outcomes and response rate calculation 11
Table 2.4: Unweighted and weighted sample profiles 13
Table 3.1: Profile of businesses in follow-up qualitative survey 17

1 Overview

This annex supplements a main report covering a 2017 survey with UK businesses on cyber security for the Department for Culture, Media and Sport (DCMS). It provides the technical details of the survey and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.[1]

1.1 Summary of methodology

There were two strands to the survey:

- A random probability telephone survey of 1,523 UK businesses was undertaken from 24 October 2016 to 11 January 2017.
- A total of 30 in-depth interviews were undertaken in January and February 2017 to follow up with businesses that had participated in the survey and gain further qualitative insights.

1.2 Strengths and limitations of the 2017 survey

While there have been other business surveys on cyber security 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. The 2017 survey shares all the same strengths of the methodology employed in 2016:

- the use of random-probability sampling to avoid selection bias
- the inclusion of micro and small businesses, which ensures that the findings are representative of the whole UK business population and not skewed towards larger businesses
- a telephone data collection approach, which aims to also include businesses 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).

[1] A copy of the main findings report and other documents can be found on the GOV.UK website, at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.

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:

- When it comes to estimates of spending and costs associated with cyber security, this survey still ultimately depends on self-reported figures from businesses. As the findings suggest, most businesses do not actively monitor the financial cost of cyber security breaches and the qualitative evidence suggests that they may underestimate this cost. Moreover, businesses can only tell us about the breaches that they have identified, and there may be other, unidentified breaches.

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

1.3 Comparability to the Cyber Security Breaches Survey 2016

The survey methodology is intended to be as comparable as possible to the earlier Cyber Security Breaches Survey 2016, in order to understand how approaches to cyber security are evolving over time. However, it should be noted that several questions in the 2017 survey were amended, for example with added, removed or tweaked answer options. Section 2.1 summarises these changes. In the main report, comparisons to 2016 are only made where valid (i.e. where questions were consistent).

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.

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 took place over three stages:

- stakeholder workshops and interviews involving Government, business and cyber security provider representatives across 13 organisations
- cognitive testing interviews with 10 businesses
- a pilot survey, consisting of 30 interviews.

Stakeholder research

The stakeholder research was intended to:

- clarify the key cyber security issues facing businesses today
- review the 2016 questionnaire, survey instruments and findings to assess gaps in knowledge and new question areas to be included in 2017
- explore ideas for getting more accurate spending and cost information from businesses, for example through the use of a survey microsite (see section 2.2)
- gather early thoughts on how the survey findings might best be disseminated.

Stakeholder research took place in July and August 2016. It included a cross-Government meeting chaired by DCMS, a stakeholder workshop run by Ipsos MORI and ICJS, and interviews with stakeholders unable to make it to the workshop, carried out by Ipsos MORI. Organisations represented included:

- The Cabinet Office
- The Centre for the Protection of National Infrastructure (CPNI)
- Government Communications Headquarters (GCHQ)
- The Home Office
- 6 UK industry representative bodies
- 3 professional cyber security or software organisations.

Following this stage, the 2016 questionnaire was amended with provisional new questions for testing. 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 to:

- introduce a range of attitudinal questions to understand the business culture towards cyber security (among core staff as well as senior managers)
- expand questions around cyber security training and cyber insurance

- splitting the impact question from 2016 into two questions that identify which breaches had a material outcome (e.g. a loss of data), and which breaches impacted on business performance
- add new questions to break down the financial costs associated with the most disruptive breach into the direct costs, recovery costs and long-term costs.

Cognitive testing

The cognitive testing was intended to test comprehension of the new questions for 2017 and any technical terms used (e.g. ransomware). Participants were recruited by telephone using sample purchased from the Dun & Bradstreet business directory. Recruitment quotas were applied and a £50 incentive was offered[2] to ensure different-sized businesses from a range of sectors took part. Specific quotas ensured that businesses from the finance or insurance, information or communications, manufacturing and retail sectors were included, as these sectors were either considered more likely to reach all the filtered questions (and therefore test these questions), or considered as important subgroups for the survey.

After this stage, the questionnaire was tweaked. The changes were highly question-specific, though some recurring issues included the need to avoid questions or statements that:

- were phrased speculatively (e.g. “cyber security can get in the way or our organisation’s business priorities” versus “cyber security gets in the way of our organisation’s business priorities)
- asked businesses to speculate about the attitudes of core staff or suppliers.

Pilot survey

The pilot survey was used to:

- 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)
- examine the quality of the sample.

Pilot fieldwork was undertaken between 5 and 11 October 2016. Again, quotas were applied to ensure the pilot covered different-sized businesses from a range of sectors.

The pilot sample was taken from the same sample frame used for the main stage survey (see next section). In total, 400 leads were randomly selected. Not all of these leads were used to complete the 30 pilot interviews, and 79 untouched leads were released for use in the main stage survey.

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

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

- cuts to bring the questionnaire length down to within c.22 minutes for the main stage (including removing low-priority questions and cutting down the wording for preambles)
- new pre-codes added for unprompted questions to reflect common "other" verbatim responses.

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

2.2 Survey microsite

A survey microsite was developed for testing in the pilot survey and eventual use in the main survey. This website served several purposes, including:

- providing reassurance that the survey was legitimate
- promoting the survey endorsements
- providing more information before respondents agreed to take part
- allowing respondents to prepare spending and cost data for the survey before taking part
- allowing 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 pilot and main survey questionnaires 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

Population and sample frame

The target population matched those included in 2016:

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

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

[3] These are typically under SIC 2007 category Q. The Cyber Security Breaches Survey does not currently include a large enough number of charities to analyse these as a specific subgroup, nor does it necessarily sample a representative range of charities. DCMS is undertaking additional work to explore the feasibility of including a specific sub-sample of charities in the survey in subsequent years.

[4] These are typically under SIC 2007 category P.

The sample frame 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 national 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 2016, organisations in the agriculture, forestry and fishing sectors, as well as those in the mining and quarrying sectors (SIC, 2007 categories A and B) were also excluded. Cyber security was judged to be a less relevant topic for these organisations, given their relative lack of e-commerce.

Sample selection

In total, 27,948 businesses were selected from the IDBR. This is much higher than the 13,346 businesses selected for the 2016 survey, reflecting the higher target of c.1,500 achieved interviews this time (versus 1,008 achieved in 2016).

The sample was proportionately stratified by region, and disproportionately stratified by size and sector. The disproportionate stratification by size reflects the intention to carry out subgroup analysis by the size of the business and by specific sector groupings assumed to have very different approaches to cyber security based on the 2016 survey, and anecdotally – the finance or insurance, information, communications or utilities, and manufacturing sector groupings. This would not be possible with a proportionate stratification (which would, for example, effectively exclude all medium and large businesses from the selected sample). Table 2.1 breaks down the selected sample by size and sector.

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

SIC 2007	Sector description	Micro or small (2–49 employees)	Medium (49–249 employees)	Large (250+ employees)	Total
C	Manufacturing	1,339	318	292	1,949
D, E	Utilities	141	27	28	196
F	Construction	1,640	66	60	1,766
G	Retail, wholesale or vehicle repair	2,242	253	267	2,762
H	Transportation or storage	1,228	135	86	1,449
I	Food or hospitality	1,511	170	94	1,775
J	Information or communication	7,390	244	207	7,841
K	Finance or insurance	2,462	663	375	3,500

SIC 2007	Sector description	Micro or small (2–49 employees)	Medium (49–249 employees)	Large (250+ employees)	Total
L	Real estate	389	15	23	427
M	Professional, scientific or technical	2,386	133	115	2,634
N	Administration	1,106	132	169	1,407
P	Education	201	32	26	259
Q	Health or social care	724	155	83	962
R	Entertainment	350	51	46	447
S	Services or membership organisations	549	17	8	574
	Total	**23,658**	**2,411**	**1,879**	**27,948**

Sample telephone tracing and cleaning

Not all the original sample was usable. In total, 19,960 original 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). Telephone tracing was carried out (for both business and residential numbers) to fill in the gaps where possible.

It should be noted that, before telephone tracing, the proportion of original IDBR leads with usable numbers was much lower in 2017 (29% with usable numbers) than in 2016 (42% with usable numbers). This suggests a need in future surveys to reassess likely telephone match rates and include a higher reserve sample to account for lower-than-expected match rates.

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 also been sampled for the Commercial Victimisation Survey 2016 (a separate Home Office survey with UK businesses taking place at the same time) were also removed to avoid harassing the same organisations for both surveys.

Following telephone tracing and cleaning, the usable sample amounted to 9,977 leads (excluding the 208 leads used in the pilot). Table 2.2 breaks these down by size and sector.

Table 2.2: Post-cleaning available sample by size and sector (excluding leads used in the pilot)

SIC 2007	Sector description	Micro or small (2–49 employees)	Medium (49–249 employees)	Large (250+ employees)	Total
C	Manufacturing	595	296	269	1,160
D, E	Utilities	45	27	25	97
F	Construction	369	62	54	485

SIC 2007	Sector description	Micro or small (2–49 employees)	Medium (49–249 employees)	Large (250+ employees)	Total
G	Retail, wholesale or vehicle repair	557	196	232	985
H	Transportation or storage	187	81	65	333
I	Food or hospitality	493	141	86	720
J	Information or communication	1,104	204	174	1,482
K	Finance or insurance	1,672	564	330	2,566
L	Real estate	110	14	23	147
M	Professional, scientific or technical	503	116	99	718
N	Administration	109	76	128	313
P	Education	62	24	16	102
Q	Health or social care	276	139	70	485
R	Entertainment	106	44	42	192
S	Services or membership organisations	170	14	8	192
	Total	**6,358**	**1,998**	**1,621**	**9,977**

The 9,977 usable leads for the main stage survey were randomly allocated into batches. The first batch included 4,500 leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band from the 2016 survey. In other words, more sample was selected in sector and size cells either where there was a higher target, or where response rates were lower last year. The subsequent batches each had c.500 or more leads. These were released as and when live sample was exhausted. More re-batching was carried out during fieldwork to allow for further controlled releases of additional sample. Not all 9,977 available leads were released in the main stage.

2.4 Fieldwork

Main stage fieldwork was carried out from 24 October 2016 to 11 January 2017 using a Computer-Assisted Telephone Interviewing (CATI) script. There was a break over the Christmas period from 23 December to 4 January inclusive, when no interviews took place. This was a shorter overall fieldwork period than in 2016 (c.10 weeks in 2017, versus c.12.5 weeks in 2016, each excluding the unproductive Christmas break period).

In total, 1,523 interviews were completed. The average interview length was just over 22 minutes (versus an average of 17 minutes in 2016).

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
- the glossary of unfamiliar terms.

Screening of respondents

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

- businesses with no computer, website or other online business presence (interviewers were briefed to probe fully before coding this outcome, and it was used only in a small minority of cases)
- businesses 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 business.

When it was established that the business was eligible and that this was the head office of the organisation, 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 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 piece of sample was called either a minimum of 7 times, or called until an interview was achieved, a refusal given or information obtained to make a judgment on the eligibility of that contact. Overwhelmingly (in 97% of cases, versus 83% of cases in 2016), leads were actually called more than 12 times before being marked as reaching the maximum number of tries (e.g. when respondents had requested to be called back at an early stage in fieldwork but had subsequently not been reached).

- Each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. 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 participants.
- 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.

Impact of news and media during fieldwork

Cyber security breaches are frequently featured in news and media. Fieldwork for this survey coincided with the following major UK news stories:

- Tesco Bank was the subject of a cyber attack in November 2016, which led to money being taken from about 20,000 current accounts.
- Around 100,000 TalkTalk and Post Office customers were reported to have lost internet access following a cyber attack in December 2016.
- Lloyds Bank was the subject of a cyber attack in January 2017, which stopped customers from using their online accounts.
- The Government's National Cyber Security Centre was officially launched in February 2017.

These stories are likely to have had some effect on the survey results. In particular they may have given a boost to the proportion of businesses saying they considered cyber security to be a high priority. Of course this does not make the results any less accurate, but provides a context for the findings.

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.[5]

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

Table 2.3: Fieldwork outcomes and response rate calculation

Outcome	Total
Total sample loaded	8,545
Completed interviews	1,523
Incomplete interviews	77
Ineligible leads	375
Refusals	2,531
Working numbers with unknown eligibility[6]	2,390
Unusable leads with working numbers	610
Unusable numbers	1,039
Expected eligibility	81%
Unadjusted response rate	18%
Adjusted response rate	27%

The adjusted response rate for the 2017 survey was lower than for 2016 (34%). This is likely to be for a range of different reasons:

- The response rate calculation was changed for this survey to reclassify businesses not available during the entire fieldwork period under “working numbers with unknown eligibility”. Previously they were classified as “unusable leads with working numbers”. Under the previous calculation, the 2017 adjusted response rate would have been 31 per cent.
- The overall fieldwork period was lower than in 2016, by c.2.5 weeks.

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

[6] 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.

- The average questionnaire length was 5 minutes longer in 2017, at c.22 minutes. This is likely to have led to more businesses refusing to take part.

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. This meant that ultimately no post-fieldwork editing was carried out 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 the 2017 survey.

Weighting

Rim weighting (random iterative method weighting) was applied to account where possible for non-response bias and also to account for the disproportionate sampling of businesses by size. The intention was to make the weighted data representative of the actual UK business population by size and sector.

In line with the weighting approach from 2016, non-interlocking rim weighting by size and sector was undertaken. Weighting by region was not applied but it should be noted that the final weighted data are closely aligned with the population region profile.

Table 2.4 shows the unweighted and weighted profiles of the final data by size, sector and region. SIC sectors have been combined into the sector groupings used in the main report.

As can be seen in Table 2.4, the achieved sample profile, before weighting was applied, had a large proportion of finance or insurance businesses (relative to their proportion in the business population). This occurred for a number of reasons, which will be reviewed in subsequent surveys in this series:

- The sample was already disproportionately stratified towards finance or insurance firms to achieve sufficient subgroup sample in this sector, and the effect was much stronger for this sector grouping than any other, since these businesses only make up two per cent of the business population.
- Out of the selected sample, the proportion of sample that was usable (i.e. with telephone numbers) was again skewed in favour of finance or insurance firms.
- The sample selected and issued in the initial batches in 2017 was put together based on how the sample performed in 2016. In 2016, there was an especially low response rate for finance or insurance firms. Relative to other sectors, the response rate for finance or insurance firms improved in 2017, which led to more of these firms than expected being interviewed through a random probability approach.

It is important to note that while this skew was beyond what was anticipated when considering the optimal sample profile at the outset of fieldwork, its impact on the overall effective sample size for the survey has been negligible.[7] Moreover, the weighting means that this skew does not affect the representativeness of the weighted data.

Table 2.4: Unweighted and weighted sample profiles

	Unweighted %	Weighted %
Size		
Micro or small (2–49 employees)	65%	97%
Medium (49–249 employees)	24%	3%
Large (250+ employees)	11%	1%
Sector		
Administration or real estate	6%	11%
Construction	5%	12%
Education, health or social care	9%	7%
Entertainment, service or membership organisations	6%	7%
Finance or insurance	23%	2%
Food or hospitality	6%	10%
Information, communication or utilities	9%	6%
Manufacturing	12%	7%
Professional, scientific or technical	8%	15%
Retail or wholesale	9%	14%
Transport or storage	6%	9%

[7] The effective sample size in 2017 was 709 (from an achieved unweighted sample size of 1,523), compared to 441 in 2016 (when the achieved unweighted sample size was 1,008). This represents a proportional improvement in the statistical reliability of the survey findings since 2016.

	Unweighted %	Weighted %
Region		
East Midlands	7%	7%
Eastern	9%	9%
London	17%	14%
North East	2%	3%
North West	9%	9%
Northern Ireland	4%	6%
Scotland	8%	10%
South East	16%	14%
South West	9%	12%
Wales	4%	4%
West Midlands	7%	7%
Yorkshire and Humberside	7%	6%

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 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.

Dataset

A de-identified dataset has been published in two comma-separate values (csv) files to enable further analysis. One file contains data labels and the other has data values. In this dataset, the following merged or derived variables have been included:

- merged region (region_comb) and merged sector (sector_comb), which were used for the merged region subgroup analysis in the main report
- two variables with derived values for the £ amount invested in cyber security, including imputed values when respondents answered as a percentage of turnover or of IT spending
  - one of these includes imputed values when respondents gave banded responses instead of numeric responses (investn), and this was used in the main report
  - the other excludes imputed values for banded responses (investx)
- other derived variables which include imputed values when respondents gave banded responses instead of numeric responses
  - for number of breaches experienced in the last 12 months (numb)
  - for the estimated cost of all breaches experienced in the last 12 months (cost)
  - for how long it took to deal with the most disruptive breach or attack (deal)
  - for the estimated direct results cost of the most disruptive breach or attack (damagedirx)
  - for the estimated recovery cost of the most disruptive breach or attack (damagerecx)
  - for the estimated long-term cost of the most disruptive breach or attack (damagelonx)
- 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).

3 Qualitative approach technical details

3.1 Sampling

The sample for the 30 in-depth interviews was taken from the survey. In the survey, respondents were asked whether they would be willing to be recontacted specifically for the follow-up interviews. In total, 643 (42%) agreed to be recontacted.

3.2 Recruitment and quotas

Recruitment was carried out by telephone. A £50 incentive was offered[8] to encourage participation.

Soft recruitment quotas were used to ensure that the 30 interviews included a mix of businesses:

- of different sizes, sectors and regions
- that treat cyber security as a high priority, but have not necessarily carried out staff training or instigated minimum standards for suppliers
- that have cyber insurance (including those who made a claim)
- that outsource cyber security
- that had incurred high value cyber security breaches (estimating the cost at more than £5,000) in the last 12 months.

3.3 Fieldwork

All telephone fieldwork was undertaken by the Ipsos MORI research team in January and February 2017. 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:

- how businesses go about managing cyber security risks
- what businesses thought of the information, advice and guidance available on cyber security
- why senior managers felt cyber security was important or not, and what might change attitudes or behaviour in this area
- experiences of cyber security breaches.

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

Table 3.1 shows a profile of the 30 interviewed businesses by size and sector.

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

Table 3.1: Profile of businesses in follow-up qualitative survey

SIC 2007	Sector description	Micro or small (2–49 employees)	Medium (49–249 employees)	Large (250+ employees)	Total
C	Manufacturing	1			1
D, E	Utilities				
F	Construction			1	1
G	Retail, wholesale or vehicle repair	3	1	3	7
H	Transportation or storage			2	2
I	Food or hospitality				
J	Information or communication	1	1		2
K	Finance or insurance	7	2		9
L	Real estate				
M	Professional, scientific or technical		2		2
N	Administration	1			1
P	Education	2			2
Q	Health or social care	1			1
R	Arts or entertainment	2			2
S	Services or membership organisations				
	Total	**18**	**6**	**6**	**30**

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 and case studies 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 exclude any spending on repair or recovery from breaches or attacks.

To make it easiest for you, you only need to answer in one of the following ways:

- *As a number in £s*
- *Or as a % of turnover*
- *Or as a % of total IT expenditure*

£

%
of turnover

%
of total IT expenditure

in last financial year

Do you have insurance which would cover you in the event of a cyber security breach or attack, or not?

Yes **/** No

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 in total 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 activities*
- *Goodwill compensation or discounts given to customers*

£

in last 12 months

Thank you

Appendix B: interviewer glossary

This is a list of some of the less well-known terms you and the respondent will come across during the interview. The definitions here can be read out to clarify things if respondents want this.

Term	**Where featured**	**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, Q46	Cloud computing uses a network of external servers accessed over the internet, rather than a local server or a personal computer, to store or transfer data. This could be used, for example, to host a website or corporate email accounts, or for storing or transferring data files.
Data classification	Q32	This refers to how files are classified (e.g. public, internal use, confidential etc)
Document Management System	Q32	A Document Management System is a piece of software that can store, manage and track files or documents on an organisation's network. It can help manage things like version control and who has access to specific files or documents.
Externally-hosted web services	Q46, Q48, Q49, Q50	Externally-hosted web services are services run on a network of external servers and accessed over the internet. This could include, for example, services that host websites or corporate email accounts, or for storing or transferring data files over the internet.
GCHQ	Q24 (DO NOT PROMPT)	Government Communications Headquarters – one of the main government intelligence services
IISP	Q24 (DO NOT PROMPT)	Institute of Information Security Professionals – a security body
Hacking	Q53A, Q64A, Q68 (DO NOT PROMPT)	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	Q9A, Q21 (DO NOT PROMPT), Q56A, Q75A	Intellectual property (IP) refers to the ideas, data or inventions that are owned by an organisation. This could, for example, include literature, music, product designs, logos, names and images created or bought by the organisation.
ISF	Q24 (DO NOT PROMPT)	Information Security Forum – a security body
Malware	Q31, Q53A, Q64A, Q65, Q68 (DO NOT PROMPT), Q78 (DO NOT PROMPT)	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)
Penetration testing	Q22, Q52, Q78 (DO NOT PROMPT)	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

Term	Where featured	Definition
Personally-owned devices	Q08, Q28, Q32, Q67	Personally-owned devices are things such as smartphones, tablets, home laptops, desktop computers or USB sticks that do not belong to the company, but might be used to carry out business-related activities
Phishing or social engineering	Q28	Fraudulent attempts to extract important information, such as passwords, from staff
Ransomware	Q53A, Q64A	Malicious software that blocks access to a computer system until a sum of money is paid
Removable devices	Q32	Removable devices are portable things that can store data, such as USB sticks, CDs, DVDs etc
Restricting IT admin and access rights	Q31	Restricting IT admin and access rights is where only certain users are able to make changes to the organisation's network or computers, for example to download or install software
Segregated guest wireless networks	Q31	Segregated guest wireless networks are where an organisation allows guests, for example contractors or customers, to access a wi-fi network that is cut off from what staff have access to
Table-top exercises	Q22	Table-top exercises are meetings where staff or senior managers simulate a cyber security breach or attack, then discuss and review the actions they would take for this breach or attack
Threat intelligence	Q30	Threat intelligence is where an organisation may employ a staff member or contractor, or purchase a product to collate information and advice around all the cyber security risks the organisation faces

Appendix C: questionnaire

INTERVIEWER INSTRUCTIONS IN BLUE
ROUTING/SCRIPTING INSTRUCTIONS IN GREEN ITALICS

Screener

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

Yes
No – another company name
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 important survey on behalf of the UK Government's National Cyber Security Programme about how UK businesses approach cyber security. This is a survey that is conducted annually.

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 UK Government's National Cyber Security Programme is led by the Cabinet Office.

ADD IF NECESSARY: The survey will help the Government to understand what businesses 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 business, including financially. The findings will inform Government policy and the guidance offered to businesses.

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 or someone else from the senior management team.

Would you be happy to take part in a 20-minute 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 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 2017, in order to help businesses like yours.
- Details of the survey are on the gov.uk website (www.gov.uk/government/publications/cyber-security-breaches-survey) and the Ipsos MORI website (csbs.ipsos-mori.com).

- 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), and the Institute of Chartered Accountants in England and Wales (ICAEW).

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
- 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
- 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 a link to our website for businesses, which 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 CSBS 2016

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 CSBS 2016

Q3. DELETED POST-PILOT IN CSBS 2016

ASK ALL
Q4.SIZEA
Including yourself, how many employees work in your organisation across the UK as a whole?
ADD IF NECESSARY: By that I mean both full-time and part-time employees on your payroll, as well as any working proprietors or owners.
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 working in 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 ALL
Q5A.SALESA
In the financial year just gone, what was the approximate turnover of your organisation across the UK as a whole?
ADD IF NECESSARY: the total amount received in respect of sales of goods and services.
PROBE FOR BEST ESTIMATE BEFORE CODING DK

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

ASK IF DON'T KNOW NUMERIC TURNOVER OF ORGANISATION (SALESA CODE DK)
Q5B.SALESB
Which of these best represents the turnover of your organisation across the UK as a whole in the financial year just gone?
PROBE FULLY

Less than £50,000
£50,000 to less than £100,000
£100,000 to less than £500,000
£500,000 to less than £2 million
£2 million to less than £10 million
£10 million to less than £50 million
£50 million or more
DO NOT READ OUT: Don't know
(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
A website or blog
Accounts or pages on social media sites (e.g. Facebook or Twitter)
The ability for your customers to order, book or pay for products or 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 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 1–6)
Q7.CORE
To what extent, if at all, are online services a core part of the goods or 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 directors or senior management? Is it …
READ OUT

Very high
Fairly high
Fairly low
Very low
DO NOT READ OUT: Don’t know
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST CODE)

Q9A.HIGH DELETED POST-PILOT IN CSBS 2017

ASK IF CYBER SECURITY IS A LOW PRIORITY (PRIORITY CODES 3–4)
Q10.LOW
What do you think makes cyber security a low priority for your organisation's directors or senior management?
DO NOT READ OUT
PROBE FULLY (“ANYTHING ELSE?”)

Don't know what we should be doing/too complicated
Expense/too expensive
Lack of awareness/understanding of cyber security
Never considered it before
No staff with right skills/who work in cyber security
No time/too time-consuming
Not an online business/no services online
Not had any cyber security issues/breaches/attacks before
Not relevant to our business generally

Nothing worth breaching/attacking
Outsource cyber security/leave it to security provider
Other *WRITE IN*
(MULTICODE; ALLOW DK)

ASK ALL
Q10A.RISK (EARLIER STATEMENT A REMOVED POST-PILOT IN CSBS 2017)
How much do you agree or disagree with the following statements?
READ OUT

a. Our organisation's core staff take cyber security seriously in their day-to-day work
b. The emphasis on cyber security gets in the way of our organisation's business priorities
c. I see conflicting advice on how businesses should deal with cyber security
d. I worry that the cyber security of our suppliers is probably not as good as ours

Strongly agree
Tend to agree
Neither agree nor disagree
Tend to disagree
Strongly disagree
DO NOT READ OUT: Don't know
SHOW FOR RISKe: DO NOT READ OUT: Have no suppliers
(SINGLE CODE; SCRIPT TO ROTATE STATEMENTS AND REVERSE SCALE EXCEPT FOR LAST CODE)

Q10B.LOWRISK REMOVED POST-PILOT IN CSBS 2017

ASK ALL
Q11.UPDATE
Approximately how often, if at all, are your organisation's directors 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
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.
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.
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.
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.
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 CSBS 2017

Q16B. DELETED PRE-PILOT CSBS 2017

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.
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.
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 business running
Clients/customers 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 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)

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)

Q22.EVAL

In the last 12 months, which of the following things, if any, have you done to formally evaluate the effectiveness of your spending on cyber security?
READ OUT

Measured trends in cyber security incidents or costs
Benchmarking against other organisations
Carried out return-on-investment calculations
Measured staff awareness
Monitored levels of regulatory compliance
Sought feedback from directors or senior management
Carried out active technical testing such as penetration testing
Carried out table-top exercises to test how people respond to breaches or attacks
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST 2 CODES)

ASK ALL

Q23.INSURE

Do you have insurance which would cover you in the event of a cyber security breach or attack, or not?
INTERVIEWER NOTE: THIS WAS ON THE PRE-INTERVIEW QUESTIONS SHEET
INTERVIEWER NOTE: IF DEPENDS ON TYPE OF BREACH/HAS INSURANCE THAT COVERS A PARTICULAR KIND OF BREACH, CODE YES

Yes
No
(ALLOW DK)

ASK IF HAVE INSURANCE (INSURE CODE 1)

Q23A.COVERAGE

How well, if at all, do you feel you understand what is and isn't covered by this insurance?
READ OUT

Very well
Fairly well
Not very well
Not at all well
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST CODE)

ASK IF HAVE INSURANCE (INSURE CODE 1)

Q23B.CLAIM
Have you ever made any insurance claims for cyber security breaches under this insurance before?

Yes
No
(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"

Auditors/accountants
Bank/business bank/bank's IT staff
Cyber Security Information Sharing Partnership (CISP)
External security/IT consultants/cyber security providers
gov.uk
Government's 10 Steps to Cyber Security guidance
Government intelligence services (e.g. GCHQ)
Government – other *WRITE IN*
Internet Service Provider
LinkedIn
Newspapers/media
Online searching generally/Google
Professional/trade/industry association
Police
Regulator (e.g. Financial Conduct Authority)
Security bodies (e.g. ISF or IISP)
Security product vendors (e.g. AVG, Kaspersky etc)
Specialist IT blogs/forums/websites
Within your organisation – senior management/board
Within your organisation – other colleagues or experts
Other (non-government) *WRITE IN*
(MULTICODE; ALLOW DK AND NULL)

Q24A.FINDINF DELETED POST-PILOT IN CSBS 2017

ASK IF SOUGHT GOVERNMENT INFORMATION (INFO CODES 5–8)
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 businesses 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 CSBS 2016

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

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

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

Q26A.TRAINUSE DELETED POST-PILOT IN CSBS 2017

Q26B.TRAINWHO
Who in your organisation attended any of the training, seminars or conferences over the last 12 months?
PROMPT TO CODE

Directors or senior management staff
IT staff
Staff members whose job role includes information security or governance
Other staff who are not cyber security or IT specialists
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
(MULTICODE)

ASK IF TRAINING ATTENDED (TRAIN CODES 2–3)
Q27.DELIVER
In which of the following ways, if any, has this training been delivered over the last 12 months?
READ OUT

As part of an induction process
On a regular basis outside of any induction process

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

Q28.COVER DELETED POST-PILOT IN CSBS 2017

Policies and procedures

READ OUT TO ALL
Now I would like to ask some questions about processes and procedures to do with cyber security. 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 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 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 business/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
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 3 MUST FOLLOW CODE 2)

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
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 HAVE POLICIES (MANAGE CODE 3)

Q32.POLICY

Which of the following aspects, if any, are covered within your cyber security-related policy, or policies?

READ OUT

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

Q32A.FOLLOW DELETED POST-PILOT IN CSBS 2017

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

ASK ALL

Q34.ISO

Are you aware of the International Standard for Information Security Management (ISO 27001), or not?

Yes
No
(ALLOW DK)

ASK IF AWARE OF ISO 27001 (ISO CODE 1)

Q35.IMPLEMA

Has your organisation implemented the International Standard for Information Security Management (ISO 27001), or not?

IF NOT: And are you intending to do so?

DO NOT READ OUT

Yes
No, and do not intend to do so
No, but is intending to do so
(SINGLE CODE; ALLOW DK)

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 CSBS 2017

Q40. DELETED PRE-PILOT IN CSBS 2017

Q41. DELETED PRE-PILOT IN CSBS 2017

Q42. DELETED PRE-PILOT IN CSBS 2016

Q43. DELETED PRE-PILOT IN CSBS 2016

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?

Yes
No
(ALLOW DK)

READ OUT IF USE WEB SERVICES (CLOUD CODE 1)
Now I would like to ask some questions about these externally-hosted web services.

Q47. DELETED POST-PILOT IN CSBS 2016

Q48.CRITICAL DELETED POST-PILOT IN CSBS 2017

ASK IF USE WEB SERVICES (CLOUD CODE 1)
Q49.COMMER
How much, if any, of the data stored on these externally-hosted web services do you consider to be commercially confidential? Is it …
READ OUT

All of it
Most of it
Some of it
None of it
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST CODE)

ASK IF USE WEB SERVICES (CLOUD CODE 1)
Q50.PERSON
How much, if any, of the data stored on these external services is personal data relating to your customers, staff or suppliers? Is it …
READ OUT

All of it
Most of it
Some of it
None of it
DO NOT READ OUT: Don't know
(SINGLE CODE; SCRIPT REVERSE SCALE EXCEPT FOR LAST CODE)

Q51.VALIDA DELETED POST-PILOT IN CSBS 2017 TO BE INCLUDED ONLY IN EVEN-NUMBERED YEARS

Q52.VALIDB DELETED POST-PILOT IN CSBS 2017 TO BE INCLUDED ONLY IN EVEN-NUMBERED YEARS

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 CSBS 2017

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) 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
Additional staff time to deal with the breach or attack, or to inform customers 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
Discouraged you from carrying out a future business activity you were intending to do
Complaints from customers
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)

ASK ALL
Q58.MONITOR
Do you have anything in place to monitor or estimate the financial cost of cyber security breaches or attacks to your organisation, or not?

Yes
No
(ALLOW DK)

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 CSBS 2016

Q62. DELETED PRE-PILOT IN CSBS 2017

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 CSBS 2017

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)/customer complaints
Reported/noticed by staff/contractors
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)
Former employee(s)
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 CSBS 2017

Q75. DELETED PRE-PILOT IN CSBS 2017

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 if customers 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
- 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 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 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
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)

ASK IF NOT REPORTED (REPORTA CODE 2)
Q77A.NOREPORT
What were the reasons for not reporting this breach or attack?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")

Breach/impact not significant enough
Breach was not criminal
Don't know who to report to
No benefit to our business
Not obliged/required to report breaches
Reporting won't make a difference
Too soon/haven't had enough time
Worried about reputational damage
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)
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 carried out
Changed/updated firewall/system configurations
Changed which users have admin/access rights
Created/changed backup/contingency plans
Created/changed policies/procedures
Deployed new systems
Disciplinary action
Formal post-incident review
Increased monitoring of third parties' cyber security
Increased spending on cyber security
Installed/changed/updated antivirus/anti-malware software
Outsourced cyber security/hired an external provider
Penetration testing
Recruited new staff
Other *WRITE IN*
(MULTICODE; ALLOW DK AND NULL)

Q78B.NOACT DELETED POST-PILOT IN CSBS 2017

Recontact

ASK ALL
Q79.RECON
This survey is part of a wider programme of research that Ipsos MORI is undertaking on behalf of the UK Government's National Cyber Security Programme to help them better understand and respond to organisations' cyber security concerns and needs. Would you be happy to take part in a more bespoke interview with Ipsos MORI in late January and February 2017, to further explore some of the issues from this survey? This interview would be more of a conversation on the specific issues relevant to your organisation, rather than a structured questionnaire.
ADD IF NECESSARY: Again, the Government will not know who has taken part, either in this survey or in any follow-up interview.
ADD IF NECESSARY: the interviews would last no longer than 45 minutes and those taking part would be offered a £50 cheque or a donation to the charity of their choice.

Yes
No

ASK ALL
Q80.PANELRECON
This survey will be repeated in a year's time. Your input is really important to help the Government to better understand and respond to organisations' cyber security concerns and needs, and to ensure that this survey represents all businesses, including ones like yours. Would you be happy for the Government or their appointed contractor to contact you for your views on this topic again in late 2017?

Yes
No

Appendix D: quailtative topic guide

	Timings and notes
Thank participant for taking part in the study and agreeing to be re-contacted in this phase. Introduce self and Ipsos MORI. Role of Ipsos MORI – independent research organisation. Explain the research: we are speaking again to businesses to learn more about their particular experiences in approaching and dealing with cyber security. The interview will build upon your responses given to us during the survey. No right or wrong answers. Commissioned through the Government's National Cyber Security Programme (led by the Cabinet Office) to conduct the follow-up research. Confidentiality: reassure that all responses are totally confidential and anonymous and that information about participant/business will not be passed on to anyone, including the Cabinet Office or any other Government Department. Length: maximum of 45 minutes. Get permission to digitally record – transcribe for quotes, no detailed attribution.	Welcome orientates participant, 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 and Data Protection Act guidelines).
Section 1: introduction to organisation	**2 to 3 minutes**
Please could you tell me a bit about your organisation? Probe on main activity of business, number of employees and if organisation is single or multi-site. Probe if plan on growing the business Probe on average age of company/staff/board members etc. Explore whether online services are/are not core part of the organisation (e.g. if organisation has website/ability for customers to pay online/online bank account/personal information about customers/employees).	The survey asks about the turnover of the business but may be useful to expand on this and get a sense of whether the company is expecting to grow/stay the same/decline over the next few years. This could influence the types of issues they may face and actions around cyber security.
Section 2: role within the organisation	**5 minutes**
Could you briefly describe your role? Probe on main responsibilities, type of contract, length of time in current role. Can you tell me about the structure of your team?	This section aims to understand more about the respondent, including how much of their role relates to cyber security, which department they work in, how the

	Timings and notes
How well do you think the structure works for dealing with cyber security? How does the team operate with the wider business regarding cyber security? Probe around if work in isolation, interconnected etc. IF OUTSOURCE CYBER SECURITY: Do you outsource cyber security? Can you tell me more about your outsourcing arrangements? Which aspects of cyber security are external providers responsible for? How does this compare with the aspects of cyber security that your business is directly responsible for? How much do you know about what your outsourced provider is doing for your business? Probe extent to which they trust the information provided by the contractor and if they feel they are being sold things they don't strictly need. What factors where behind the decision to outsource cyber security? Probe around breach/attack, changes in staff, external advice/information. How did you choose your contractor?	department works with the rest of the business.
Section 3: seeking information	**7 minutes**
I'm interested to find out more about the kinds of information you receive regarding cyber security. What areas have you sought information regarding cyber security? Probe if they know what information they are looking for and the extent to which they understand it. What drove you to look for information/seek advice or guidance? Probe on frequency/due to breach. How regularly do you stay updated on cyber security? Probe if linked to a specific event or general events in the news/media Do you share the information with other staff members? Probe on channels used (e.g. email, on intranet, training sessions etc). IF COME ACROSS CONFLICTING ADVICE: In the survey you told us that you had come across conflicting advice on cyber security? Can you tell us more about this? Probe around what issue/s they found conflicting advice on. What did you do in these instances?	This section explores in greater detail the information received by businesses. This helps to contextualise the factors that may be driving their decisions around cyber security. In the cognitive interviews it was mentioned that if businesses know what they are looking for then it can be easy to locate the correct guidance; those who are unsure of the specifics have more difficulty in trusting the information they receive.

	Timings and notes
How does the conflicting advice make you think about cyber security? IF AWARE OF GOVERNMENT SOURCES: Are you aware of any government information on cyber security? Probe if actively sought the information or if came across it. What did you do with the government information that you found? How helpful did you find the government information? Did they meet your needs? How could it be improved? ASK ALL Are there any sources you would trust more than others? (e.g. software/security firms/government information) Are you aware of the Data Protection Act 1998? How does your company currently adhere to the Data Protection Act? Are you aware of the new General Data Protection Regulations and what this means for your business? What measures have you put in place to adhere to the changes?	
Section 4: business culture around cyber security	**10 minutes**
I would like to understand more about your business culture and attitudes towards cyber security. Can you tell me about the importance of cyber security in the organisation you work? Explore further extent to which consider high/low priority from the survey Do you think cyber security gets in the way of organisation's business priorities? Can you tell me about your staffs' attitudes towards cyber security? Probe on extent to which senior management consider it a high/low priority and how this impacts on staff/different grades. How aware do you think the staff are about cyber security issues? IF HAVE SUPPLIERS: Can you tell me what you know about your suppliers' attitudes towards cyber security? What information do you share with your suppliers/distributors? Probe around sharing cyber security capabilities/ attacks/ vulnerabilities identified including reasons why they do/don't share.	This section aims to understand more about the business culture and attitudes towards cyber security.

	Timings and notes
Do you worry about your suppliers' capabilities to deal with cyber security? Probe reasons. Does your company ensure that your suppliers/distributors adhere to any cyber security standards or good practice guides? Is this part of their contractual obligations? Who is involved in setting these standards? How often are these contractual obligations reviewed? Do you know if your company would still work with a supplier/distributor if it did not have the capabilities to deal with cyber security? Do you have any involvement in the decision of appointing suppliers? If YES: probe what involvement/input into the guidelines. What input would you recommend someone in your position has on appointing suppliers/distributors? IF VIEW CYBER SECURITY AS A LOW BUSINESS PRIORITY: What are the factors that contribute to cyber security being considered a low priority? Probe if gets in the way of other business priorities. What would have to happen for cyber security to be a higher priority? What do you think could happen to your company if there was a cyber security breach? Probe around possible impact. Do you think you know what your company needs to put in place to deal with cyber security?	
Section 5: training	**6 to 8 minutes**
Does your company provide cyber security training? IF PROVIDE STAFF TRAINING: Who attends training? Probe around board/senior management, middle-management, other employees etc. What are staff attitudes to training? What difference does training make? Probe on impact of board members, senior staff, contract workers and employees. What do you consider the benefits of having training? Is the training compulsory of voluntary? Do the staff have enough/right training to be confident in doing their job? How could the training be improved?	This section aims to provide contextual information about the training that the company provides and who attends training on cyber security.

	Timings and notes
Do you feel you have the training/expertise to deal with cyber security breaches? How often does the training get reviewed? Probe around when breach happens/quarterly basis. If they deal with cyber security as part of job role, are they involved in designing the training for the staff? IF CONSIDER CYBER SECURITY A HIGH PRIORITY AND DO NOT HAVE STAFF TRAINING: In the survey you mentioned that cyber security is a high priority to your organisation's directors or senior management. What are the factors that contribute to cyber security being considered a high priority? Explore reasons around not investing in cyber security, specifically not investing in training. What are the reasons for not having cyber security training? Do you think you know what your company needs to do to deal with cyber security? What do you think are the benefits of having cyber security training? What would incentivise your company to start training on cyber security? EVERYONE ELSE NOT PROVIDING STAFF TRAINING: What are the reasons for not having cyber security training? What do you think are the benefits of having cyber security training? What would incentivise your company to start training on cyber security?	
Section 6: insurance	**6 to 8 minutes**
Do you currently have insurance which would cover you in the event of a cyber security breach or attack? IF HAVE INSURANCE: Can you tell me what you know about the policy you have? Probe whether cyber security is part of their insurance package or stand alone, type of cover (1st or 3rd party losses) What do you consider the benefits of the insurance? What factors where behind the decision to get insurance? Probe if got insurance after breach/received advice/competitors have it.	This section looks at awareness and attitudes around cyber insurance, and explores the experiences of those who have made a claim on their insurance.

	Timings and notes
Did you/someone else in the organisation request this in the policy? Did you/someone else compare different insurance policies? How did the policies vary? Probe on what was covered/differences in cost/other differences across providers. Did you have to fulfil specific criteria to get cyber security insurance? Probe around ease of getting an insurer. Does the insurance protect in circumstances where companies haven't taken appropriate precautions (e.g. ISO27001)? IF MADE A CLAIM ON INSURANCE: How would you describe your experience in making a claim? Probe around challenges/ease. What information did you have to provide when you submitted your claim? Probe around how the information was found. Who from your organisation was involved in the process of submitting a claim? Was your claim successful? Probe around length to get resolved. How has the claim impacted on the cost of your insurance? IF DO NOT HAVE INSURANCE: What are the reasons for not having cyber security insurance? Probe if believe insurance is necessary, costly, complicated. In the next 5 years, do you think you will get cyber security insurance? Why/why not? What factors would make you consider getting cyber security insurance?	
Section 7: experience of breaches	**10 minutes**
IF HAVE HAD CYBER SECURITY BREACHES Can you tell me how this/these breaches occurred? Probe on extent to which were staff-related/external/international/accidental How disruptive was this/these breaches? Do you know what the attackers were specifically looking for (e.g. data, IP or simply being destructive)? Did they manage to obtain this? How well do you think your company dealt with the breach? Probe about what worked well/what didn't	This section is asked of those who have experienced breaches. Aim of this section is to examine participants' responses to cyber security breaches in more depth.

	Timings and notes
What did you learn when dealing with the cyber security breach? Probe what the business learnt from the experience of breach/any best practice from suppliers/competitors How has this informed your approach for dealing with cyber security? Do you know what the gaps are in your approach to dealing with breaches, if any? Can you tell me what actions you took as a consequence of the breaches? Probe on the steps taken/any advice sought from experts/consultants Does your company have policies and an incident response plan to deal with the impact of breaches? If so who is involved Was the plan followed? Probe how effective the plan was Do you inform your customers/suppliers/stakeholders/shareholders about breaches? Probe the circumstances around this if depends on the breach Thinking about all the breaches you have had, how have these informed your cyber security policy? Have any of the breaches impacted the future plans of your business in relation to dealing with cyber security (new tools/systems to monitor/estimate loss, strategic business plan, future investment)?	
Section 8: cyber security in future (only if time)	**5 minutes (only if time)**
I would like to ask you about your business and cyber security plans over the coming years. Where do you see the business in the next 5 years? Explore plans for online services in future. Over the next 5 years, what cyber security issues do you expect your company could face? What has been put in place to deal with cyber security? Probe on hiring more staff/training/changing company policy. Do you think your company's approach will be effective? What support or guidance do you think you will need to deal with cyber security? Probe on where they will go to seek the support.	A brief section to understand where the company views the challenges regarding cyber security in the next few years and if they think they are in a good place to deal with them.
Section 9: wrap-up	**2 to 3 minutes**

	Timings and notes
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? Confirm incentive details: To thank you for your time, we would like to offer a cheque for £50 to either yourself or a charity of your choosing. Please could you tell me who you would like the cheque to be made out to? And what address should we post it to? Reassure about confidentiality. THANK AND CLOSE	Wrap up interview, summarise suggestions for further support/guidance

Department
for Culture
Media & Sport

4th Floor, 100 Parliament Street
London, SW1A 2BQ
www.gov.uk/dcms