HM Government

Ipsos MORI
Social Research Institute

University of Portsmouth

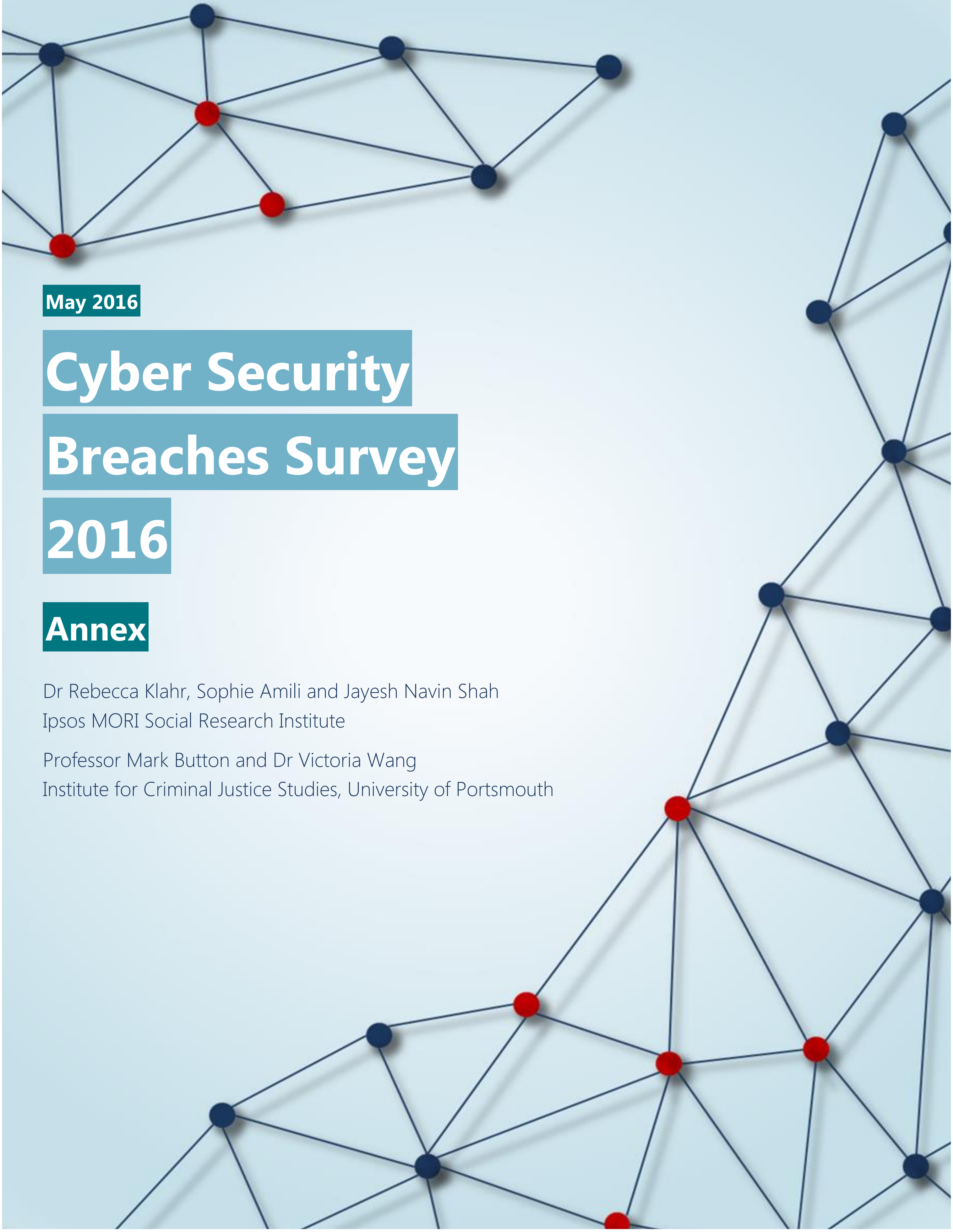
May 2016

Cyber Security Breaches Survey 2016

Annex

Dr Rebecca Klahr, Sophie Amili and Jayesh Navin Shah
Ipsos MORI Social Research Institute

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



Contents

List of Tables

1 Overview

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

1.1 Summary of methodology

There were two strands to the research:

- A random probability telephone survey of 1,008 UK businesses was undertaken from 30 November 2015 to 5 February 2016.
- A total of 30 in-depth interviews were undertaken in January and February 2016 to follow up businesses that had participated in the survey and gain further qualitative insights.

1.2 Strengths and limitations of this research

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, this research is intended to be statistically representative of UK businesses of all sizes and all relevant sectors.

In summary, the relative strengths of this research are:

- 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 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 costs from reputational damage and opportunity costs).

At the same time, while this research 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 research 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 research 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 research 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 Information Security Breaches Surveys

From 2012 to 2015, the Government commissioned and published a series of Information Security Breaches Surveys. While these surveys covered similar topics to this Cyber Security Breaches Survey, 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 are not possible.

This change in methodology reflects the respective priorities for the two sets of surveys. The Information Security Breaches Surveys were primarily focused on examining trends over time and took a pragmatic approach to this – the broad trends observed in those surveys can still be considered valid. The Cyber Security Breaches Survey aims to provide as accurate and representative a picture of all UK businesses as possible, while also providing new benchmarks against which to track changes over time in future surveys.

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 the Department for Culture, Media and Sport (DCMS). Development took place over three stages:

- interviews and discussions with stakeholders from 17 organisations
- cognitive testing interviews with 10 businesses
- a pilot survey, consisting of 25 interviews.

Stakeholder research

The stakeholder research was intended to:

- clarify the key cyber security issues facing businesses today
- explore how to find the most appropriate individual to interview within a business
- explore how to minimise non-response and improve the accuracy of responses, especially around the impact of cyber security breaches
- gather early thoughts on how the survey findings might best be disseminated.

Stakeholder research took place from 7 September to 19 October 2015. Stakeholders either attended a face-to-face meeting set up by DCMS on 7 September 2015 or took part in a 45-minute telephone interview with a researcher from Ipsos MORI or ICJS. Organisations represented included:

- 2 Government Departments
- 6 policing bodies
- 3 UK industry representative bodies
- 3 professional cyber security or software organisations
- 2 large businesses (250 or more employees) and 1 small business (10 to 49 employees).[1]

Following this stage, an initial questionnaire was drafted, alongside a reassurance email and pre-interview questions sheet (see Appendix A for a copy). The latter two survey instruments were intended to improve the response rate, as well as the coverage and accuracy of responses around cyber security spending and costs.

Cognitive testing

The cognitive testing was intended to test:

- comprehension of the questions and any technical terms used

[1] Businesses were recruited from ICJS contacts. The small business also took part in a cognitive testing interview.

- the user-friendliness of the reassurance email and the pre-interview questions sheet.

Participants were recruited by telephone using sample purchased from the Dun & Bradstreet business directory, as well as ICJS contacts. 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, and retail sectors were included, as these sectors were considered more likely to reach all the filtered questions (and therefore test these questions).

After this stage the questionnaire and other survey instruments were tweaked. The main changes included:

- making the questionnaire better suited to businesses that outsourced cyber security or did not take much action around the topic (to avoid quits from these businesses)
- creating a glossary for interviewers to help explain technical terms (see Appendix B for a copy)
- giving respondents flexibility to answer questions on cyber security spending as a percentage of turnover, or a percentage of IT spending, as alternatives to a £ amount.

Pilot survey

The pilot survey was used to:

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

Pilot fieldwork was undertaken between 12 and 18 November 2015. 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, 445 leads were randomly selected. Not all of these leads were used to the 25 pilot interviews, and 252 untouched leads were released for use in the main stage survey.

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

- cuts to bring the questionnaire length down to within c.20 minutes for the main stage
- new precodes added for unprompted questions to reflect common "other" verbatim responses
- response bands at the spending and cost questions were expanded to start off lower (e.g. "less than £500" rather than "less than £1,000"), reflecting the low answers that most respondents were giving.

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

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

2.2 Sampling

Population and sample frame

The target population included:

- private companies with more than one person on the payroll
- charities 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.

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 research 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.

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, 13,346 businesses were selected from the IDBR, with proportionate stratification by region and sector, and disproportionate stratification by size. The disproportionate stratification by size reflects the intention to carry out subgroup analysis by the size of the business. This would not be possible with a proportionate stratification (which would effectively exclude all medium and large businesses from the selected sample). Table 2.1 breaks down the selected sample by size and sector.

[3] These are typically under SIC 2007 category Q.

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

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	336	365	248	**949**
D, E	Utilities	39	25	24	**88**
F	Construction	851	152	0	**1,003**
G	Retail, wholesale or vehicle repair	770	231	160	**1,161**
H	Transportation or storage	188	113	70	**372**
I	Food or hospitality	673	214	134	**1,022**
J	Information or communication	1,997	309	321	**2,627**
K	Finance or insurance	1,123	332	335	**1,789**
L	Real estate	210	40	25	**274**
M	Professional, scientific or technical	738	198	155	**1,091**
N	Administration	534	302	210	**1,046**
P	Education	96	62	65	**223**
Q	Health or social care	317	269	84	**671**
R	Entertainment	128	56	59	**243**
S	Services or membership organisations	366	25	0	**391**
	Total	**8,366**	**2,694**	**2,286**	**13,346**

Sample telephone tracing and cleaning

Not all the original sample was usable. In total, 7,420 original leads had no telephone number, while 359 further leads had 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.

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.

Following telephone tracing and cleaning, the usable sample amounted to 6,513 leads (excluding the 196 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	150	313	224	**687**
D, E	Utilities	12	23	19	**54**
F	Construction	253	123	0	**376**
G	Retail, wholesale or vehicle repair	324	192	141	**657**
H	Transportation or storage	46	92	62	**200**
I	Food or hospitality	236	156	119	**511**
J	Information or communication	208	240	300	**748**
K	Finance or insurance	718	277	320	**1315**
L	Real estate	55	37	22	**114**
M	Professional, scientific or technical	164	161	123	**448**
N	Administration	126	237	176	**539**
P	Education	35	52	55	**142**
Q	Health or social care	113	248	71	**432**
R	Entertainment	38	43	48	**129**
S	Services or membership organisations	136	25	0	**161**
	Total	**2,614**	**2,219**	**1,680**	**6,513**

The 6,513 usable leads for the main stage survey were randomly allocated into batches of c.2,000 or more leads, with batches to be released as and when live sample was exhausted. The batches were proportionate to the original selection targets by size and sector. More re-batching was carried out during fieldwork to allow for further controlled releases of additional sample. Not all 6,513 available leads were released in the main stage.

2.3 Fieldwork

Main stage fieldwork was carried out from 30 November 2015 to 5 February 2016 using a Computer-Assisted Telephone Interviewing (CATI) script. There was a break over the Christmas period from 24 December to 4 January inclusive, when no interviews took place.

In total, 1,008 interviews were completed. The average interview length was just over 17 minutes.

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 (this code was ultimately not used).

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. Typically (in 83% of cases), leads were actually called more than 12 times (e.g. when respondents had requested to be called back at an early stage in fieldwork but had subsequently not been reached).

- Each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. 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) and the Institute of Chartered Accountants in England and Wales (ICAEW).

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

While cyber security breaches are frequently featured in news and media, it is worth noting that fieldwork for this survey coincided with three cyber security breaches on UK companies that received relatively widespread media coverage. In October 2015, in the lead up to the survey launch, the TalkTalk website was hacked. In December, JD Wetherspoon had a similar attack. Most recently, in January 2016, HSBC had a denial-of-service attack taking down its online banking service.

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.

2.4 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	4,155

[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).

Outcome	Total
Completed interviews	1,008
Incomplete interviews	39
Ineligible leads	207
Refusals	831
Working numbers with unknown eligibility[6]	1,559
Unusable leads with working numbers	511
Unusable numbers	389
Expected eligibility	72%
Adjusted response rate	34%

2.5 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 had overwhelmingly found the SIC 2007 codes in the sample to be accurate.

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.

[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.

Various interlocking and non-interlocking weights were tested to see how closely the final data matched the population profile and also to ensure the achieved weighting efficiency still enabled subgroup analysis by size and sector (given that more complex weights would negatively impact the weighting efficiency). Ultimately, 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.

Table 2.4: Unweighted and weighted sample profiles

	Unweighted %	**Weighted %**
Size		
Micro or small (2–49 employees)	45%	97%
Medium (49–249 employees)	35%	3%
Large (250+ employees)	20%	1%
Sector		
Manufacturing	10%	7%
Utilities	1%	1%
Construction	7%	12%
Retail, wholesale or vehicle repair	11%	18%
Transportation or storage	4%	5%
Food or hospitality	9%	10%
Information or communication	9%	6%
Finance or insurance	7%	2%
Real estate	2%	3%
Professional, scientific or technical	10%	12%
Administration	11%	11%
Education	2%	2%
Health or social care	8%	5%
Entertainment	3%	1%
Services or membership organisations	5%	7%
Region		
East Midlands	6%	7%
Eastern	10%	10%
London	17%	15%
North East	3%	3%

	Unweighted %	Weighted %
North West	7%	7%
Northern Ireland	5%	6%
Scotland	10%	10%
South East	16%	16%
South West	9%	8%
Wales	4%	5%
West Midlands	8%	8%
Yorkshire and Humberside	6%	7%

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 gave numeric responses. It was agreed with DCMS that for those who gave banded responses, a numeric response would be imputed. This ensured that no survey data went unused and also allowed for larger sample sizes for these questions.

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

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

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

SPSS dataset

A de-identified SPSS dataset has been published to enable further analysis. 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 of the last 12 months (deal)
  - for the estimated cost of the most disruptive breach or attack of the last 12 months (damage)

- 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 this follow-up research. In total, 395 (39%) agreed to be recontacted.

3.2 Recruitment and quotas

Recruitment was carried out by telephone. A £50 incentive was offered[7] 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 considered e-commerce to be core to their business or not
- that treat cyber security as a low or high priority
- with or without formal cyber security policies
- that had or had not incurred cyber security breaches in the last 12 months.

Minimum recruitment quotas were also used to recruit at least four interviews respectively with businesses:

- aware of Government-backed initiatives such as Cyber Essentials or the 10 Steps guidance
- saying they have cyber security insurance
- that outsource cyber security or use external training providers
- that say their staff use personal devices for carrying out regular business-related activities
- that have incurred reputational damage from cyber security breaches in the last 12 months.

3.3 Fieldwork

All telephone fieldwork was undertaken by the Ipsos MORI research team in January and February 2016. Interviews lasted around 45 minutes on average.

The interview topic guide was drafted by Ipsos MORI and was approved by DCMS. 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.

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

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

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

SIC 2007	Sector description	Micro or small (2–49 employees)	Medium (49–249 employees)	Large (250+ employees)	Total
C	Manufacturing	1		2	**3**
D, E	Utilities				
F	Construction		1		**1**
G	Retail, wholesale or vehicle repair	2			**2**
H	Transportation or storage	1			**1**
I	Food or hospitality	1	1		**2**
J	Information or communication	2	2		**4**
K	Finance or insurance		3		**3**
L	Real estate	1	1		**2**
M	Professional, scientific or technical	2			**2**
N	Administration		1	2	**3**
P	Education		1		**1**
Q	Health or social care	1	3	1	**5**
R	Entertainment				
S	Services or membership organisations	1			**1**
	Total	**12**	**13**	**5**	**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

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
- New measures needed to prevent or protect against future breaches or attacks
- 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

£
in last 12 months

And thinking 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, how much, if anything, did this cost your organisation financially?

£
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	Q28	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	Q28	This refers to how files are classified (e.g. public, internal use, confidential etc).
Document Management System	Q28	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	Q40–Q46, Q56	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	Q21 (DO NOT PROMPT)	Government Communications Headquarters – one of the main government intelligence services
IISP	Q21 (DO NOT PROMPT)	Institute of Information Security Professionals – a security body
Intellectual property	Q18 (DO NOT PROMPT), Q46, Q56	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	Q21 (DO NOT PROMPT)	Information Security Forum – a security body
Malware	Q27, Q46, Q56, Q57, Q60, Q70	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	Q19, Q45, Q70 (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.
Personally-owned devices	Q05, Q24, Q28, Q46, Q56, Q59	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	Q24	Fraudulent attempts to extract important information, such as passwords, from staff

Term	Where featured	Definition
Removable devices	Q28	Removable devices are portable things that can store data, such as USB sticks, CDs, DVDs etc
Restricting IT admin and access rights	Q27	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	Q27	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	Q19	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	Q26	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

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
(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 2016, 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-2016) and the Ipsos MORI website (www.ipsos-mori.com/cybersecurity).
- The survey has been endorsed by the Confederation of British Industry (CBI), the Federation of Small Businesses FSB) and the Institute of Chartered Accountants in England and Wales (ICAEW).

Yes
Wants more information by email SEND REASSURANCE EMAIL
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 some pre-interview questions, which I recommend looking at. 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 interview.

READ OUT TO ALL
First, I would just like to ask some general questions about your organisation.

ASK ALL
Q1.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
WRITE IN RANGE 2–500,000
(SOFT CHECK IF >99,999; ALLOW DK)

ASK IF DON'T KNOW SIZE OF ORGANISATION (SIZEA CODE DK)
Q2.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
Q3.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 business bank account your organisation pays into
ONLY SHOW IF SAMPLE SICVAR=1: An industrial control system
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)
Q4.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
Q5.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)

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
Q6.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)

ASK IF CYBER SECURITY IS A LOW PRIORITY (PRIORITY CODES 3–4)
Q7.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
Q8.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)

ASK ALL
Q9.INVESTA
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
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)
Q10.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)
Q11.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)
Q12.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 (INVESTED CODE DK)
Q13.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)

ASK IF ANSWERING AS A PERCENTAGE OF TURNOVER AND INVEST IN CYBER SECURITY (INVESTD CODE>0 OR NULL OR INVESTE CODES 1–7)
Q16a.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; ALLOW DK)

ASK IF DON'T KNOW NUMERIC TURNOVER OF ORGANISATION (SALESA CODE DK)
Q16b.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 IF ANSWERING AS A PERCENTAGE OF OVERALL IT EXPENDITURE (INVESTA CODE 3)
Q14.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)
Q15.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)
Q16.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)
Q17.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)
Q18.REASON
What are the main reasons that your organisation invests in cyber security?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")
INTERVIEWER NOTE: IF "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 company-owned data/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)
Q19.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
Q20.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 ALL
Q21.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"

Business bank/bank's IT staff
Cyber Security Information Sharing Partnership (CISP)
External security/IT consultants
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)
Within your organisation – senior management/board
Within your organisation – other colleagues or experts

Other (non-government) WRITE IN
(MULTICODE; ALLOW DK AND NULL)

ASK ALL
Q22.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)

ASK IF TRAINING ATTENDED (TRAIN CODES 2–3)
Q23.DELIVER
In which of the following ways, if any, has this cyber security 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)

ASK IF SEMINARS OR TRAINING ATTENDED (TRAIN CODES 1–3)
Q24.COVER
Which of the following aspects, if any, were covered in any of the cyber security training, seminars or conferences attended over the last 12 months?
READ OUT

General awareness, culture or attitudes around cyber security
Fraudulent attempts to extract important information, such as passwords, from staff (sometimes called social engineering or phishing)
Use of email, web browsers or social networks
Remote or mobile working
Use of personally-owned devices for business activities
What to do if you spot a cyber security breach or attack
The impact or cost of cyber security 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 STATEMENTS)

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
Q25.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 ALL
Q26.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
Q27.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
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)
Q28.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)

ASK ALL
Q29.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)

ASK ALL
Q30.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)
Q31.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)
Q32.10STEPS
Are you aware of the government's 10 Steps to Cyber Security guidance, or not?

Yes
No
(DP AUTO-CODE 1 IF INFO CODE 5; ALLOW DK)

ASK ALL
Q33.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)
Q34.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)

ASK IF NOT IMPLEMENTED CYBER ESSENTIALS (IMPLEMB NOT CODES 1–3)
Q35.PLAN
Do you plan to implement the Cyber Essentials scheme in the next 12 months, or not?

Yes
No
(ALLOW DK)

ASK IF FULLY IMPLEMENTED CYBER ESSENTIALS (IMPLEMB CODES 1–2)
Q36.BADGE
And has your organisation been badged for having implemented [IF IMPLEMB CODE 1: Cyber Essentials; IF IMPLEMB CODE 2: Cyber Essentials Plus], or not?

Yes – badged
No – not badged
(ALLOW DK)

ASK IF NOT BADGED (BADGE CODE 2)
Q37.APPLY
Do you plan to apply for the [IF IMPLEMB CODE 1: Cyber Essentials; IF IMPLEMB CODE 2: Cyber Essentials Plus] badge in the next 12 months, or not?

Yes
No
(ALLOW DK)
ASK ALL
Q38.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)
Q39.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)

ASK ALL
Q40.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.

ASK IF USE WEB SERVICES (CLOUD CODE 1)
Q41.CRITICAL
How critical, if at all, are these externally-hosted web services to your organisation?
READ OUT

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

ASK IF USE WEB SERVICES (CLOUD CODE 1)
Q42.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)
Q43.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)

ASK IF USE WEB SERVICES (CLOUD CODE 1)
Q44.VALIDA
Over the last 12 months, have you taken any steps to test or validate the security of the external providers of these services, or not?

Yes
No
(ALLOW DK)

ASK IF VALIDATED SECURITY OF EXTERNAL PROVIDERS (VALIDA CODE 1)
Q45.VALIDB
Which of the following, if any, have you done over the last 12 months to test or validate the security of the external providers of these services?
READ OUT

Ensured any contracts with providers included cyber security requirements
Audited the provider's security
Ensured the provider is certified as ISO 27001 compliant
Ensured all data held on these services are encrypted
Obtained a service auditor's report (e.g. ISAE 3402) on the provider's controls
Carried out penetration testing to check the provider's security
Required the provider to match your organisation's security standards
Requested reports from the provider on security breaches that might affect your data
Having a contingency plan in case the provider ceases operation or you wish to exit
DO NOT READ OUT: Don't know
(MULTICODE; SCRIPT ROTATE LIST EXCEPT FOR LAST CODE)

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.]

ASK ALL
Q46.BREACH
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

ONLY SHOW IF ONLINE CODE 2: Denial-of-service attacks that take down your website
People accessing computers, networks or servers without permission (i.e. hacking)
Money stolen electronically (e.g. through online banking)
Money stolen through fraudulent emails or fake websites
Personal information (e.g. customer data) stolen electronically
People damaging or stealing software from your computers or network, even if accidentally
People downloading unlicensed or stolen software to your computers or network, even if accidentally
Computers becoming infected with viruses, spyware or malware
Theft of intellectual property
Others impersonating your organisation in emails or online
ONLY SHOW IF CLOUD CODE 1: Any breaches or attacks relating to an externally-hosted web service
Any breaches or attacks relating to personally-owned devices being used for business activities
Any breaches or attacks relating to social media sites (e.g. Facebook or Twitter)
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)

ASK IF ANY BREACHES OR ATTACKS (BREACH CODES 1–14)
Q47.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)
Q48.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)
Q49.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 (BREACH CODES 1–14)
Q50.IMPACT
Thinking of all the cyber security breaches or attacks experienced in the last 12 months, have these 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
Lost or stolen assets
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
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
Q51.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 (BREACH CODES 1–14)
Q52.COSTA
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.
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)
Q53.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)

ASK IF HAD REPUTATIONAL DAMAGE (IMPACT CODE 8)
Q54.REPUT
You mentioned that you had incurred reputational damage from the cyber security breaches or attacks experienced over the last 12 months. What was the nature of the reputational damage incurred?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")

Complaints from customers
Complaints from shareholders
Complaints from suppliers
Less trust in our industry sector
Loss of customers/less trusting/less willing to buy from us
Loss of suppliers/less trusting/less willing to work with us
Lowered share price
Negative coverage on social media (Facebook, Twitter etc)
Negative coverage on traditional media (TV, radio, press etc)
PR costs incurred
Staff morale/behaviour lowered
Other WRITE IN
(MULTICODE; ALLOW DK)

ASK ALL
Q55.INCID
Do you have any formal cyber security incident management processes, or not?

Yes
No
(ALLOW DK)

READ OUT IF MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE BREACH CODES 1–14)
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.

ASK IF MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE BREACH CODES 1–14)
Q56.DISRUPT
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 BEST DESCRIBES THE KIND OF BREACH OR ATTACK

ONLY SHOW IF ONLINE CODE 2: Denial-of-service attacks that take down your website
People accessing computers, networks or servers without permission (i.e. hacking)
Money stolen electronically (e.g. through online banking)
Money stolen through fraudulent emails or fake websites
Personal information (e.g. customer data) stolen electronically
People damaging or stealing software from your computers or network, even if accidentally
People downloading unlicensed or stolen software to your computers or network, even if accidentally
Computers becoming infected with viruses, spyware or malware
Theft of intellectual property

Others impersonating your organisation in emails or online
ONLY SHOW IF CLOUD CODE 1: Any breaches or attacks relating to an externally-hosted web service
Any breaches or attacks relating to personally-owned devices being used for business activities
Any breaches or attacks relating to social media sites (e.g. Facebook or Twitter)
Any other types of cyber security breaches or attacks
(SINGLE CODE; SCRIPT ONLY SHOW CODES MENTIONED AT BREACH; DP AUTO-CODE SAME CODE FROM BREACH IF ONLY 1 CODE MENTIONED; ALLOW DK)

READ OUT IF EXPERIENCED ONE TYPE OF BREACH OR ATTACKS MORE THAN ONCE ([ONLY 1 BREACH CODES 1–14] AND [FREQ CODES 2–6 OR DK])
You mentioned you had experienced [INSERT RESPONSE FROM BREACH] 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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q57.IDENTB
IF ONE TYPE OF BREACH OR ATTACK EXPERIENCED ONLY ONCE ([ONLY 1 BREACH CODES 1–14] 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 BREACH CODES 1–14] 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 BREACH CODES 1–14): PROMPT IF NECESSARY WITH BREACH OR ATTACK MENTIONED EARLIER: [INSERT RESPONSE FROM BREACH]
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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q58.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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q59.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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q60.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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q61.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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q62.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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q63.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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q64.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)
Q65.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)

ASK IF ONE TYPE OF BREACH OR ATTACK EXPERIENCED MORE THAN ONCE OR MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED AND CAN CONSIDER A PARTICULAR BREACH OR ATTACK, AND INCURRED COSTS FROM BREACHES OR ATTACKS ([{ONLY 1 BREACH CODES 1–14 AND FREQ CODES 2–6 OR DK} OR DISRUPT NOT DK] AND [COSTA CODE NOT NULL])
Q66.DAMAGEA
[IF COSTB CODE 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}.] Approximately how much, if anything, do you think this particular breach or attack cost your organisation financially? This includes any of the direct and indirect costs or damages you mentioned earlier.
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

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 AND REF)
(DP AUTO-CODE ANSWER FROM COSTA IF [ONLY 1 BREACH CODES 1–14] AND FREQ CODE 1; DP AUTO-UPDATE ANSWER AT COSTA TO MATCH DAMAGEA IF DAMAGEA>COSTA)

ASK IF DON’T KNOW TOTAL COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEA CODE DK)
Q67.DAMAGEB
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; DP AUTO-CODE ANSWER FROM COSTB IF COSTA DK AND [ONLY 1 BREACH CODES 1–14] AND FREQ CODE 1; DP AUTO-UPDATE ANSWER AT COSTA TO DK AND COSTB TO MATCH DAMAGEB IF [TOP OF DAMAGEB CODE]>[ANSWER AT COSTA OR TOP OF COSTB CODE])

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q68.REPORTA
Was this breach or attack reported to anyone outside your organisation, or not?

Yes
No
(ALLOW DK)

ASK IF REPORTED (REPORTA CODE 1)
Q69.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)
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)
Was publicly declared
Website administrator

Other government agency
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 BREACH CODES 1–14] OR DISRUPT NOT DK)
Q70.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)

ASK ALL
Q71.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 2016, 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

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

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

About Ipsos MORI's Social Research Institute

The Social Research Institute works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. This, combined with our methodological and communications expertise, helps ensure that our research makes a difference for decision makers and communities.