Department for Digital, Culture, Media & Sport

Ipsos MORI

Cyber Security Breaches Survey 2020

Technical annex

This technical annex supplements a main statistical release by the Department for Digital, Culture, Media and Sport (DCMS), covering the Cyber Security Breaches Survey 2020 results for businesses and charities. It can be found on the GOV.UK website, alongside infographic summaries of the findings, at: https://www.gov.uk/government/collections/cyber-security-breaches-survey.

This annex provides the technical details of the 2020 quantitative survey (fieldwork carried out in winter 2019) and qualitative element (carried out in early 2020), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

A separate annex, available on the same GOV.UK page, summarises the results from the smaller survey of education institutions, carried out for the first time this year.

The Cyber Security Breaches Survey is a quantitative and qualitative study of UK businesses and charities. It helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the government to shape future policy in this area.

For this latest release, the quantitative survey was carried out in winter 2019 and the qualitative element in early 2020.

Responsible analyst:

Emma Johns
07990602870

Statistical enquiries:

cyber.survey@culture.gov.uk
@DCMSinsight

General enquiries:

enquiries@culture.gov.uk

Media enquiries:

020 7211 2210

Contents

Chapter 1: Overview

1.1 Summary of methodology

The Cyber Security Breaches Survey 2020 comprised:

- a quantitative random probability telephone survey of 1,348 UK businesses, 337 UK registered charities and 287 education institutions, carried out from 9 October 2019 to 23 December 2019
- 30 qualitative in-depth interviews with businesses and charities that took part in the quantitative survey, undertaken in January and February 2020.

1.2 Strengths and limitations of the survey

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

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

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

The 2020 survey shares the same strengths as previous surveys in the series:

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

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

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

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

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

1.3 Changes from previous waves

One of the objectives of the survey is to understand how approaches to cyber security and the cost of breaches are evolving over time. Therefore, the survey methodology is intended to be as comparable as possible to the 2016, 2017, 2018 and 2019 surveys.

The 2020 survey is also methodologically consistent with previous years. However, in order to reduce the overall scale of this year's study, in line with DCMS's requirements, there we more significant changes to the scope, in terms of questionnaire lengths and sample sizes:

- We reduced the number of business interviews from c.1,500 in previous years to 1,348 this year. Similarly, we reduced the charity sample from c.500 in previous years to 337 this year. This allowed DCMS to include a separate sample of 287 education institutions, surveyed for the first time this year – the findings for which are reported separately to the main statistical release in another annex.[1]
- We reduced the average questionnaire lengths from c.22 minutes to c.17 minutes. This reflected that some of the content was no longer relevant to DCMS's policy objectives and needed to be removed to allow space for new topics.

The following two changes also apply this year.

- We changed the weighting approach this year to more accurately reflect the balance of micro vs. small firms in the weighted data. We explain this in more detail in Section 2.6. The main statistical release still looks at changes over time, as analysis of the impact of the changes in weighting suggests that they make a negligible impact on the findings.
- There were two script omissions this year that affect the TYPE and OUTCOME questions. Analysis suggests that there is some impact on the OUTCOME question's comparability to findings published in previous years. We have, therefore, revised the trend data reported in the main statistical release at this question. We discuss these omissions, and the implications, in the main findings report as well as Section 2.7.

1.4 Comparability to the earlier Information Security Breaches Surveys

From 2012 to 2015, the government commissioned and published annual Information Security Breaches Surveys.[2] 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

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

[2] See https://www.gov.uk/government/publications/information-security-breaches-survey-2015 for the final survey in this series. This was preceded by earlier surveys in 2014, 2013 and 2012. We reiterate that these surveys are not representative of all UK businesses and are not comparable to the Cyber Security Breaches Survey series.

different for both sets of surveys. This means that comparisons between surveys from both series are not possible.

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

Ipsos MORI developed the questionnaire and all other survey instruments (e.g. the interview script and respondent microsite), which DCMS then approved. Development for this year's survey took place over three stages from July to September 2019:

- stakeholder engagement, including industry and government stakeholders
- cognitive testing interviews with four businesses and four charities
- a pilot survey, consisting of 30 interviews (7 businesses, 15 charities and 8 education institutions).

A full list of all questionnaire amends since 2019 is included at the end of this section.

Stakeholder engagement and initial questionnaire review

Ipsos MORI had a series of conversations (by telephone and email) with stakeholders including the Association of British Insurers (ABI), the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB) and the Institute of Chartered Accountants in England and Wales (ICAEW). These represent the organisations that have been engaged with the survey since its inception.

In these conversations, we gathered feedback on any new questions or areas of interest raised in the 2019 survey, any new topics for discussion for 2020 and the wider context on how stakeholders use the data from the survey.

Before this stage, the DCMS team had already liaised with various government stakeholders about the survey, such as the Home Office, Government Communications Headquarters (GCHQ) and the National Cyber Security Centre (NCSC). Based on these discussions, the feedback from industry stakeholders, and their own internal thinking, DCMS decided to make the following changes to the questionnaire:

- We added new questions to explore insurance (INSUREX and INSUREYES), audits (IDENT), supplier risks (SUPPLYRISK) and incident response (INCIDCONTENT) in more depth than in previous years, reflecting on some of the key findings from the 2019 qualitative research around these topics. The previous questions on these topics were removed as a result.
- We removed or replaced certain categories from the questions about organisations' digital footprints (ONLINE) and the technical rules and controls they have in place for their cyber security (RULES). This included:
    - removing categories at ONLINE measuring whether organisations had websites or staff email addresses, as these are ubiquitous across all organisations
    - rephrasing or removing categories at RULES considered to be confusion or open to misinterpretation, such as network firewalls, guest Wi-Fi, passwords and two-factor authentication.
- In order to make way for the new question areas and with a view to reducing the overall length of the questionnaire, DCMS opted to cut the following questionnaire sections, which were no longer relevant for their policy objectives:
    - all questions associated with investment in cyber security, which had previously achieved very broad estimates with wide margins of error (SALESA, SALESB, SALESDUM, INVESTA, INVESTB, INVESTC, INVESTD, INVESTE, INVESTF, INVESTG, ITA, ITB and REASON)

- outsourcing (OUTSOURCING) of cyber security, which is already covered elsewhere in the questionnaire
- questions related to skills gaps and training (ATTITUDES, TRAIN and TRAINWHO), which are now explored in separate DCMS research[3]
- certain questions on the nature of cyber security breaches or attacks that only achieved very broad estimates or relatively speculative answers in previous years (LENGTH, NUMBA, NUMBB, FACTOR, SOURCE, INTENT, DEALA and DEALB)
- a question on the presence of cloud networks (CLOUD)
- questions on the General Data Protection Regulation, or GDPR (GDPRFINE, GDPRREP, GDPRAWARE, GDPRCYBER and GDPRWHAT), which is also a topic being explored in separate DCMS research, with publication forthcoming.

Cognitive testing

The Ipsos MORI research team carried out eight cognitive testing interviews with businesses and charities to test comprehension of new questions for 2020. At this stage, DCMS had not yet decided to include a sample of education institutions, which is why these organisations were not included in the cognitive testing.

We recruited all participants by telephone. We purchased the business sample from the Dun & Bradstreet business directory, and took a random selection of charities from the charity regulator databases in each UK country. We applied recruitment quotas and offered £50 incentive[4] to ensure different-sized organisations from a range of sectors or charitable areas took part.

After this stage, the questionnaire was tweaked. The changes were very minor, tweaking wording for the categories at questions like INSUREX, IDENT and RULES.

We had also tested further questions on insurance (around reasons for buying cyber insurance) and supplier risks (e.g. around specific actions taken to address supplier risks and barriers to addressing supplier risks). These were considered too complex for the quantitative survey and were instead set aside as topics for the qualitative stage.

After the cognitive testing but before the pilot survey, DCMS requested the inclusion of a small sample of education institutions (primary schools, secondary schools, and further and higher education institutions) to be included in this year's survey. With this in mind, we made some further minor changes to adapt the questionnaire for their inclusion, for example adding in breaches caused by students at the TYPE question (types of breaches or attacks identified).

Pilot survey

The pilot survey was used to:

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

Ipsos MORI interviewers carried out all the pilot fieldwork between 25 September and 1 October 2019. Again, we applied quotas to ensure the pilot covered different-sized businesses from a

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

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

range of sectors, charities with difference incomes and from different countries, and the various education institutions we intended to survey in the main fieldwork. This was with one exception – we excluded any higher education sample, as the population of universities is so small (making the available sample precious). We carried out 22 interviews, breaking down as:

- 7 businesses
- 15 charities
- 3 primary schools
- 3 secondary schools
- 2 further education colleges

The pilot sample came from the same sample frames used for the main stage survey (see next section). In total, we randomly selected 292 business leads, 296 charity leads and 80 education institution leads.

The questionnaire length for the pilot was 23 minutes, which was above target for the main stage. Following feedback from the pilot survey, we made some changes to the questionnaire deleting more questions on supplier risks and GDPR.

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

Full list of questionnaire changes since the 2019 survey

The following questions were amended and are no longer comparable with previous years:

- INSUREX
- RULES3
- RULES9.

The following question which were present in the 2019 SPSS data have been removed. In some cases, we have kept the variable with blank data to preserve the numeric ordering of variables in the file (e.g. since there is an ONLINE3 variable, we have kept ONLINE1 and ONLINE2 rather than delete them). We have then relabelled these variables to make it clear they are no longer being used.

- ONLINE1 to ONLINE2
- OUTSOURCE
- ATTITUDE1 to ATTITUDE4
- REASON1 to REASON28
- NOINSURE1 to NOINSURE19
- TRAIN1 to TRAIN5
- TRAINWHO1 to TRAINWHO7
- NOPOL1 to NOPOL22
- IDENT1 to IDENT3
- TENSTEPS
- ESSENT
- IMPLEMB
- SUPPLY
- ADHERE1 to ADHERE8
- CLOUD
- NUMBA, NUMBB and NUMB
- INCID
- LENGTH
- FACTOR1 to FACTOR23
- SOURCE1 to SOURCE19
- INTENT
- DEALA, DEALB and DEAL

- GDPRFINE
- GDPRPREP
- GDPRAWARE
- GDPRCHANGE
- GDPRCYBER
- GDPRWHAT1 to GDPRWHAT28
- SALES
- INVESTN_BANDS.

The following questions or variables were added:

- INSUREYES1 to INSUREYES6
- INFO54 (new code, based on verbatim responses)
- SCHEME1 to SCHEME5
- SUPPLYRISK1 to SUPPLYRISK2
- IDENT9 to IDENT11
- RULES17
- TYPE13
- INCIDCONTENT1 to INCIDCONTENT8
- IDENTB22 to IDENTB24 (new codes, based on verbatim responses)
- REPORTB31 to REPORTB34 (new codes, based on verbatim responses)
- PREVENT34 to PREVENT35 (new codes, based on verbatim responses).

2.2 Survey microsite

As in previous years, a publicly accessible microsite[5] (still active as of April 2020) was again used to:

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

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

2.3 Sampling

Business population and sample frame

The target population of businesses matched those included in the all the previous surveys in this series:

- private companies or non-profit organisations[6] with more than one person on the payroll

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

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

- independent schools or colleges.[7]

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

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

A handful of universities had been included in this sample in previous years. However, they were actively omitted this year, since they were instead included in the separate education institutions sample.

Exclusions from the IDBR sample

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

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

Charity population and sample frames (including limitations)

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

- the Charity Commission for England and Wales database: http://data.charitycommission.gov.uk/default.aspx
- the Office of the Scottish Charity Regulator database: https://www.oscr.org.uk/about-charities/search-the-register/charity-register-download
- the Charity Commission for Northern Ireland database: https://www.charitycommissionni.org.uk/charity-search/.

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

Therefore, while the Charity Commission in Northern Ireland database was the best sample frame for this survey, it cannot be considered as a truly random sample of Northern Ireland

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

charities at present. In 2020, there were 6,118 registered charities on the Northern Ireland database, compared to 6,078 in 2019.

Education institutions population and sample frame

The education institutions sample frame came from two sources:

- the Get Information about Schools[8] government database, which contains a list of all state-funded primary schools and secondary schools (including free schools, academies, Local Authority-maintained schools and special schools), colleges and universities in England
- online lists of all UK universities – to be able to add those in Wales, Scotland and Northern Ireland to the sample.

This was the first time that we included a sample of education institutions in the survey. DCMS considered this sample as an experimental aspect of the overall survey. Given the significant differences in size and management approaches between different types of education institutions, we split the sample frame into three independent groups:

- 17,576 primary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 5 to 11)
- 3,617 secondary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 11+)
- 429 further education colleges (270) and universities (159).

Sample selection

In total, 79,031 businesses were selected from the IDBR for the 2020 survey. This is similar to the 77,432 selected in 2019. However, it is much higher than the 53,783 businesses selected for the 2018 survey, and the 27,948 selected in the 2017 survey. We chose to keep the higher number to ensure there was enough reserve sample to meet the size-by-sector survey targets, based on the sample quality of previous waves. For example, in the 2018 survey, we had used up all reserve sample in the largest size band. There had also been a successive decline in sample quality in previous years (in terms of telephone coverage and usable leads). Ultimately, the 2020 sample quality turned out to be marginally better than the 2019 sample (with a higher proportion of usable leads), leaving us with sufficient usable leads.

The business sample was proportionately stratified by region, and disproportionately stratified by size and sector. An entirely proportionately stratified sample would not allow sufficient subgroup analysis by size and sector. For example, it would effectively exclude all medium and large businesses from the selected sample, as they make up a very small proportion of all UK businesses – according to the Business Population Estimates 2019, published by the Department for Business, Energy and Industrial Strategy (BEIS).[9] Therefore, we set disproportionate sample targets for micro (1 to 9 staff), small (10 to 49 staff), medium (50 to 249 staff) and large (250 or more staff) businesses. We also boosted specific sectors, to ensure we could report findings for the same sector subgroups that were used in the 2019 report. The boosted sectors included:

- financial and insurance
- health, social work or social care
- information and communications
- professional, scientific and technical

[8] See https://get-information-schools.service.gov.uk/.

[9] See https://www.gov.uk/government/statistics/business-population-estimates-2019.

- wholesale and retail trade.

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

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

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

SIC 2007 letter[10]	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
B, C, D, E	Utilities or production (including manufacturing)	1,202	237	336	683	2,458
F	Construction	7,967	149	113	135	8,364
G	Retail or wholesale (including vehicle sales and repairs)	4,671	418	232	794	6,115
H	Transport or storage	5,883	152	203	285	6,523
I	Food or hospitality	3,971	443	213	189	4,816
J	Information or communications	14,747	301	196	289	15,533
K	Finance or insurance	994	271	345	295	1,905
L, N	Administration or real estate	7,861	249	238	434	8,782
M	Professional, scientific or technical	11,740	227	204	450	12,621
P	Education	3,030	233	107	118	3,488
Q	Health, social care or social work	4,318	292	303	255	5,168
R, S	Entertainment, service or membership organisations	2,895	151	116	96	3,258
	Total	**69,279**	**3,123**	**2,606**	**4,023**	**79,031**

The charity sample was proportionately stratified by country and disproportionately stratified by income band, using the respective charity regulator databases to profile the population. This used the same reasoning as for businesses – without this disproportionate stratification, analysis by income band would not be possible as hardly any high-income charities would be in the selected sample. In addition, having fewer high-income charities in the sample would be likely to reduce the variance in responses, as high-income charities tend to take more action on cyber security than low-income ones. This would have raised the margins of error in the survey estimates.

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

As the entirety of the three charity regulator databases were used for sample selection, there was no restriction in the amount of charity sample that could be used, so no equivalent to Table 2.1 is shown for charities.

Similarly, the entirety of the Get Information about Schools database was available for sample selection, so no equivalent table is shown for education institutions.

Sample telephone tracing and cleaning

Not all the original sample was usable. In total, 69,168 original business leads had either no telephone number or an invalid telephone number (i.e. the number was either in an incorrect format, too long, too short or a free phone number which would charge the respondent when called). For Scottish charities, there were no telephone numbers at all on the database. We carried out telephone tracing (matching the database to both the UK Changes business and residential number databases) to fill in the gaps where possible. The selected sample was also cleaned to remove any duplicate telephone numbers.

No telephone tracing was required for charities from England and Wales, and Northern Ireland, nor for any of the education institutions. In these sample frames, there was already very high or comprehensive telephone number coverage.

At the same time as this survey, Ipsos MORI was also carrying out another business survey with a potentially overlapping sample – the Commercial Victimisation Survey 2020 for the Home Office. We therefore removed overlapping sample leads from this survey to avoid contacting the same organisations for multiple surveys, and minimise respondent burden.

Following telephone tracing and cleaning, the usable business sample amounted to 25,693 leads. For the Scotland charities sample, 2,710 leads had telephone numbers after matching.

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

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

SIC 2007 letter	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
B, C, D, E	Utilities or production (including manufacturing)	488	171	308	620	1,587
		41%	72%	92%	91%	65%
F	Construction	2,574	99	102	126	2,901
		32%	66%	90%	93%	35%
G	Retail or wholesale (including vehicle sales and repairs)	1,522	277	204	712	2,715
		33%	66%	88%	90%	44%
H	Transport or storage	1,107	103	186	250	1,646
		19%	68%	92%	88%	25%
I	Food or hospitality	800	190	169	172	1,331
		20%	43%	79%	91%	28%

SIC 2007 letter	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
J	Information or communications	3,143	149	160	245	3,697
		21%	50%	82%	85%	24%
K	Finance or insurance	591	219	303	254	1,367
		59%	81%	88%	86%	72%
L, N	Administration or real estate	1,902	121	188	379	2,590
		24%	49%	79%	87%	29%
M	Professional, scientific or technical	3,086	129	184	370	3,769
		26%	57%	90%	82%	30%
P	Education	927	128	95	105	1,255
		31%	55%	89%	89%	36%
Q	Health, social care or social work	1,001	169	281	232	1,683
		23%	58%	93%	91%	33%
R, S	Entertainment, service or membership organisations	885	89	93	85	1,152
		31%	59%	80%	89%	35%
	Total	**18,026**	**1,844**	**2,273**	**3,550**	**25,693**
		26%	**59%**	**87%**	**88%**	**33%**

The usable leads for the main stage survey were randomly allocated into separate batches for businesses and charities. The first business batch included 5,466 leads proportionately selected to incorporate sample targets by sector and size band, and response rates by sector and size band from the 2019 survey. In other words, more sample was selected in sectors and size bands where there was a higher target, or where response rates were relatively low last year. The first charity batch had 1,016 leads matching the disproportionate targets by income band.

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

2.4 Fieldwork

Ipsos MORI carried out all main stage fieldwork was from 9 October 2019 to 23 December 2019 using a Computer-Assisted Telephone Interviewing (CATI) script. This was a similar overall fieldwork period as for the 2019 survey.

In total, we completed 1,348 interviews with businesses, and 337 with charities. The average interview length was 17 minutes for businesses and 17 minutes for charities.

Fieldwork preparation

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

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

Screening of respondents

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

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

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

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

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

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

Random-probability approach and maximising participation

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

- Each organisation loaded in the main survey sample was called either a minimum of 7 times, or until an interview was achieved, a refusal given, or information obtained to make a judgment on the eligibility of that contact. Overwhelmingly (in 95% of cases), leads were called 10 times or more before being marked as reaching the maximum number of tries. For example, this outcome was used when respondents had requested to be called back at an early stage in fieldwork but had subsequently not been reached.
- Each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. Evening and weekend interviews were also offered if the respondent preferred these times.

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

- Interviewers could send the reassurance email to prospective respondents if the respondent requested this.
- The survey had its own web page on the government's GOV.UK and Ipsos MORI websites, to let businesses know that the contact from Ipsos MORI was genuine. The web pages included appropriate Privacy Notices on processing of personal data, and the data rights of participants, following the introduction of GDPR in May 2018.
- The survey was endorsed by the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), the Institute of Chartered Accountants in England and Wales (ICAEW), the Association of British Insurers (ABI), the Charity Commission for England and Wales and the Charity Commission for Northern Ireland meaning that they allowed

their identity and logos to be used in the survey introduction and on the microsite, to encourage businesses to take part.

- As an extra encouragement, we offered to send respondents an electronic copy of the survey findings, and a help card listing the range of government guidance on cyber security, following their interview. A copy of this help card is included as Appendix D.
- Specifically to encourage participation from universities, DCMS and Ipsos MORI jointly requested that Jisc (a membership organisation of individuals in digital roles within the higher education sector) send out an email to their membership promoting the survey.

Fieldwork monitoring

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

2.5 Fieldwork outcomes and response rate

We monitored fieldwork outcomes and response rates throughout fieldwork, and interviewers were given regular guidance on how to avoid common reasons for refusal. Table 2.3 shows the final outcomes and the adjusted response rate calculations for businesses and charities.[11]

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

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

Outcome	Total for businesses	Total for charities
Total sample loaded	8,420	900
Completed interviews	1,348	337
Incomplete interviews	29	9
Ineligible leads – established during screener[12]	220	7
Ineligible leads – established pre-screener	90	29
Refusals[13]	1,790	156

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

[12] Ineligible leads were those found to be sole traders, public sector organisations or the small number of organisations that self-identified as having no computer, website or online interaction. Those falling in the latter self-identified category were probed by interviewers to check this was really the case.

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

Outcome	Total for businesses	Total for charities
Unusable leads with working numbers[14]	1,453	121
Unusable numbers[15]	64	2
Working numbers with unknown eligibility[16]	3,448	278
Expected eligibility of screened respondents[17]	86%	98%
Expected eligibility of working numbers[18]	59%	74%
Unadjusted response rate	16%	33%
Adjusted response rate	27%	45%
Cooperation rate[19]	43%	66%

The adjusted response rate for businesses in the 2020 survey was significantly higher than for 2019 (23%), representing an improvement in the overall administration of the survey and potentially also reflecting the lower average interview length after cutting the questionnaire (17 minutes, vs. 22 minutes in 2019). Several steps have been taken each year to reduce these barriers to taking part, including reassurances around confidentiality, survey endorsements and setting up the survey microsite.

The target number of interviews for education institutions was very small – a total of c.300 interviews spread across three independent sample groups (primary schools, secondary schools, and further and higher education institutions). Eligibility for these samples was 100%. Therefore, we have simply presented the unadjusted response rates, which are as follows:

- 31% for primary schools (108 interviews from a sample of 566)
- 20% for secondary schools (72 interviews from a sample of 534)
- 17% for further education colleges and universities (35 interviews from a sample of 207).

It should be noted that the further and higher education institution sample is made up of 8 further education colleges and 27 universities.

[14] This includes sample where there was communication difficulty making it impossible to carry out the survey (either a bad line, or language difficulty), as well as numbers called 10 or more times over fieldwork without ever being picked up.

[15] This is sample where the number was in a valid format, so was loaded into the main survey sample batches, but which turned out to be wrong numbers, fax numbers, household numbers or disconnected.

[16] 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.

[17] Expected eligibility of screened respondents has been calculated as: (completed interviews + incomplete interviews) / (completed interviews + incomplete interviews + leads established as ineligible during screener). This is the proportion of refusals expected to have been eligible for the survey.

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

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

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 costs and time spent dealing with breaches. If respondents gave unusually high or low answers at these questions relative to the size of their organisation, the interviewer would read out the response they had just recorded and double-check this is what the respondent meant to say. This meant that, typically, no post-fieldwork editing has been required to remove outliers.

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

We did not undertake SIC coding. Instead the SIC 2007 codes that were already in the IDBR sample were used to assign businesses to a sector for weighting and analysis purposes. The pilot survey in 2017 had overwhelmingly found the SIC 2007 codes in the sample to be accurate, so this practice was carried forward to subsequent surveys.

Weighting (businesses and charities)

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

We did not weight by region, primarily because region is not considered to be an important determining factor for attitudes and behaviours around cyber security. Moreover, the final weighted data are already closely aligned with the business population region profile. The population profile data came from the BEIS Business Population Estimates 2019.[9]

Non-interlocking rim weighting by income band and country was undertaken for charities. The population profile data for these came from the respective charity regulator databases.

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

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

Table 2.4: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Micro (1–9 staff)	48%	82%
Small (10–49 staff)	21%	15%
Medium (50–249 staff)	16%	3%
Large (250+ staff)	16%	1%
Sector		
Administration or real estate	12%	13%
Construction	11%	13%
Education	2%	1%
Entertainment, service or membership organisations	5%	7%
Finance or insurance	9%	2%
Food or hospitality	8%	10%
Health, social care or social work	9%	4%
Information or communications	9%	6%
Professional, scientific or technical	11%	15%
Retail or wholesale (including vehicle sales or repairs	12%	18%
Transport or storage	3%	4%
Utilities or production (including manufacturing)	11%	7%

Table 2.5: Unweighted and weighted sample profiles for charity interviews

	Unweighted %	Weighted %
Income band		
£0 to under £10,000	28%	38%
£10,000 to under £100,000	15%	34%
£100,000 to under £500,000	17%	13%
£500,000 to under £5 million	22%	6%
£5 million or more	10%	1%
Unknown income	8%	8%
Country		
England and Wales	84%	85%
Northern Ireland	3%	3%
Scotland	13%	12%

Changes to the weighting approach for businesses in 2020

The overall weight criteria for businesses – non-interlocking rim weighting by size and sector – have been consistent in each year of the survey. In previous years, the size weights have been split into three categories:

- micro and small combined (1–49 staff)
- medium (50–249 staff)
- large (250+ staff).

However, the sampling approach implemented since 2017 (covered in Section 2.3), boosts the relative proportion of small businesses in the unweighted sample compared to the population proportion. Therefore, the corresponding weighting approach has typically led to weighted samples that have slightly overrepresented small businesses and underrepresented micro businesses in the final data.

This year, we trialled two sets of weights. The first set continued the same weighting approach taken in previous years while the second set added separate weight categories for micro and small businesses. The second set of weights is an improved approach, in that it more accurately reflects the proportions of micro businesses vs. small businesses in the population. After trialling both approaches, we compared them to see what impact the new weights had on the data. Across all questions, we found a negligible impact on the results. We therefore decided, in agreement with DCMS, to use the new weighting approach this year.

Strictly speaking, the change in weighting approach would typically mean that estimates from this year's survey are no longer directly comparable to previous years. In practice, however, we believe these comparisons are still valid given the negligible impact that changing the weights has on the data. Therefore, in the main statistical release, we make straightforward comparisons between the 2020 data with this new weighting and previous years of data with the old weighting. In our approach to testing for statistically significant differences over time, we have assumed that the data are comparable across years. All testing is carried out using the effective sample size, which accounts for the impact of the weighting.

Table 2.6 shows the four business sizes bands and their proportions in the weighted sample, both under the new (chosen) weighting scheme and the original (rejected) weighting scheme.

Table 2.6: Current and previous size weighting schemes compared

	New weights %	Original weights %
Micro (1–9 staff)	82%	71%
Small (10–49 staff)	15%	26%
Medium (50–249 staff)	3%	3%
Large (250+ staff)	1%	1%

Table 2.7 shows the results for the proportion of businesses identifying breaches and prioritisation of breaches under the new weights and the original (rejected) weights.

Table 2.7: Impact of current weighting scheme on percentage scores for key questions

	New weights	Original weights
% identifying any breaches or attacks in the last 12 months (overall)	49%	46%
% identifying any breaches or attacks in the last 12 months (micro businesses)	43%	43%
% identifying any breaches or attacks in the last 12 months (small businesses)	62%	62%
% saying cyber security is a very or fairly high priority for senior managers (overall)	81%	80%
% saying cyber security is a very or fairly high priority for senior managers (micro businesses)	78%	78%
% saying cyber security is a very or fairly high priority for senior managers (small businesses)	86%	86%

Representativeness of the education institutions sample

The education institution samples are unweighted. They were surveyed as simple random samples, with no clear variables for stratification.

With this in mind, the primary and secondary school samples might be considered as broadly representative. However, with the achieved samples being relatively small compared to the size of their populations, we believe the results are best treated as indicative. They are unlikely to represent the full variation within these populations.

The further education college and university sample is extremely small (35 interviews) and merges together two independent populations in a way that does not reflect the balance of further education colleges vs. universities. This was done to produce a larger sample size that allows for better de-identification of the data and better indicative analysis. However, it means that the results from this sample should be considered as highly indicative and not representative. They give a broad insight into these two populations and how they might compare against UK businesses.

It is important to remember that our school samples and the sample of further education colleges come from England only (i.e. not including Wales, Scotland or Northern Ireland). This reflects the fact that education policy is devolved across the UK – and the database we used for sampling the school and college populations was the England-only Get Information about Schools government database.

Derived variables

For the questions in the survey estimating the financial costs of breaches, respondents were asked to give either an approximate numeric response or, if they did not know, then a banded response. The vast majority (typically around 8 in 10) of those who gave a response (excluding refusals) gave numeric responses. We agreed with DCMS from the outset of the survey that for those who gave banded responses, a numeric response would be imputed, in line with all previous surveys in the series. This ensures that no survey data goes unused and also allows for larger sample sizes for these questions.

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

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

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

Associated datasets

A de-identified SPSS dataset will also be published on the UK Data Archive to enable further analysis. The variables are consistent with those in the 2019 and 2018 survey datasets, outside of new questions.

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

- the estimated cost of all breaches experienced in the last 12 months (cost_bands)
- the estimated direct results cost of the most disruptive breach or attack (damagedirx_bands)
- the estimated recovery cost of the most disruptive breach or attack (damagerecx_bands)
- the estimated long-term cost of the most disruptive breach or attack (damagelonx_bands)
- the sum-total of estimated costs of the most disruptive breach or attack, merging responses across damagedirx, damagerecx and damagelonx (damage_bands).

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

- merged region (region_comb), which includes collapsed region groupings to ensure that no individual respondent can be identified
- a merged sector variable (sector_comb2), which matches the sector groupings used in the 2020 and 2019 main reports

No region groupings are included for the education institution data, to avoid the risk of these schools, colleges or universities being identified.

Rounding differences between the SPSS dataset and published data

If running analysis on weighted data in SPSS, users must be aware that the default setting of the SPSS crosstabs command does not handle non-integer weighting in the same way as typical survey data tables.[20] Users may therefore see very minor differences in results (no more than one percentage point, and on rare occasions) between the SPSS dataset and the

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

percentages in the main release and infographics, which consistently use the survey data tables.

2.7 Points of clarification on the data

Sector grouping before the 2019 survey

In the SPSS datasets for 2016 to 2018, an alternative sector variable (sector_comb1) was included. This variable grouped some sectors together in a different way, and was less granular than the updated sector variable (sector_comb2).

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

The previous grouping reflected how we used to report on sector differences before the 2019 survey. As this legacy variable has not been used in the report for the last two years, we have stopped including it in the SPSS dataset, in favour of the updated sector variable.

Omission of answer categories in 2020

This year, response categories at two questions were omitted from the business and charity interviews due to a script error. These were:

- "attacks that try to take down your website or online services" at TYPE (types of breaches or attacks identified in the last 12 months)
- "your website or online services were taken down or made slower" at OUTCOME (the material outcomes of breaches or attacks).

This means that this year's survey did not explicitly record denial-of-service attacks.

The impact of this omission at TYPE (attacks that try to take down your website or online services) on the wider data and trends is expected to be negligible. In order to test this, we have recreated the trend data for the proportions identifying any breaches or attacks for previous years with this response category excluded, and we found no changes in the figures. This reflects the fact that, in previous years of the survey, there were only ever a handful of organisations that identified denial-of-service attacks as their only type of cyber security breach.

The omission at OUTCOME (your website or online services were taken down or made slower) is expected to have had some impact. A total of 10 per cent of the businesses and 9 per cent of the charities identifying breaches or attacks gave this response in 2019. Around half of these said it was the only material outcome from their breaches or attacks. Therefore, if this category had been included, we expect that the proportion of businesses and charities saying their breaches or attacks had resulted in a material outcome would have been c.4 to 5 percentage points higher, based on past trends.

When reporting data from previous years in the main findings report from the TYPE and OUTCOME questions, we have revised these trend data to exclude the omitted codes. Therefore, we are still making a like-for-like comparison across years. However, it means that any TYPE and OUTCOME figures from past years presented in the 2020 main statistical release will differ from those that were presented in previous years' reports.

Chapter 3: Qualitative approach technical details

3.1 Sampling

We took the sample for the 30 in-depth interviews from the quantitative survey. We asked respondents during the quantitative survey whether they would be willing to be recontacted specifically to take part in a further 45-minute interview on the same topic as the survey. In total, 592 businesses (43%) and 158 charities (51%) agreed to be recontacted.

Ultimately, we carried out 21 interviews with businesses and 9 with charities.

In previous years, we typically carried out around 50 in-depth interviews with businesses and charities. This year, we reduced it to 30 as part of an overall reduction in the scope of the business and charities research, to allow DCMS to fund the new, experimental research with education institutions. The reduced number of interviews this year does not materially change the strength of the insights we are able to produce.

3.2 Recruitment quotas and screening

We carried out recruitment for the qualitative element by telephone, using a specialist business recruiter. We offered a cheque or charity donation made on behalf of participants for £50 to encourage participation.

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

- that had insurance that covers cyber security risks
- that had previously considered supplier-related cyber security risks
- that said they undertake internal or external audits covering cyber security
- that had experienced a cyber security breach but not acted on it.

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

We also briefed the recruiter to carry out a further qualitative screening process of participants, to check that they felt capable of discussing at least some of the broad topic areas covered in the topic guide (laid out in the following section). The recruiter probed participants' job titles, job roles, and gave them some further information about the topic areas over email. The intention was to screen out organisations that might have been willing to take part but would have had little to say on these topics.

3.3 Fieldwork

The Ipsos MORI research team carried out all fieldwork in January and February 2020. We conducted 30 interviews by telephone. Interviews lasted around 45 minutes on average.

DCMS originally laid out their topics of interest for 2020. Ipsos MORI then drafted the interview topic guide around these topics, which was reviewed and approved by DCMS. The qualitative topic guide has changed each year much more substantially than the quantitative questionnaire, in order to respond to the new findings that emerge from each year's quantitative survey. The intention is for the qualitative research to explore new topics that were not necessarily as big or

salient in previous years, as well as to look more in depth at the answers that organisations gave in this year's survey. This year, the guide covered the following broad question areas:

- How have things changed in how organisations approach cyber security? Have organisations gone from being reactive to breaches to proactive to stopping them? What planned changes do they have?
- Who is responsible for managing the cyber security risks posed by suppliers? How do organisations manage risk in the supply chain? What kind of standards are organisations enforcing on suppliers and how adequate do they feel these are?
- What are the more and less important drivers behind having cyber insurance? Are there any positive behavioural impacts from having cyber insurance? Why do businesses not have cyber insurance? Would they ever consider it?
- What does an audit involve? Why do they do them? How often do they undertake audits? Who gets involved? What are the differences between internal and external audits?
- Why are organisations not taking action on certain breaches? What kind of breach requires action? What kind does not?
- What motivates organisations to report breaches? Why are they not reporting breaches? Who do they report breaches to? What support do they need?
- What are organisations' main sources of information and guidance on cyber security? What type of information or guidance is considered most useful? What do they think of government information and guidance in particular?

There was not enough time in each interview to ask about all these topics, so we used a modular topic guide design, where the researcher doing the interview would know beforehand to only focus on a selection of these areas. Across the course of fieldwork, the core research team reviewed the notes from each interview and gave the fieldwork team guidance on which topics needed further coverage in the remaining interviews. This ensured we asked about each of these areas in a wide range of interviews, with at least 6 interviews covering each topic.

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

Tables 3.1 and 3.2 shows a profile of the 21 interviewed businesses by size and sector.

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

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

SIC 2007 letter	Sector description	Total
Q	Health, social care or social work	3
R, S	Entertainment, service or membership organisations	0
	Total	**21**

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

Size band	Total
Micro or small (1–49 staff)	11
Medium (49–249 staff)	5
Large (250+ staff)	5

Table 3.3 shows a profile of the 9 interviewed charities by income band.

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

Income band	Total
£0 to under £10,000	2
£10,000 to under £100,000	0
£100,000 to under £500,000	0
£500,000 to under £5 million	3
£5 million or more	3
Unknown income	1

3.4 Analysis

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

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

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
When it comes to cyber security insurance, which of the following best describes your situation? ..... *A. We have a specific cyber security insurance policy* *B. We do not currently have a specific cyber security insurance policy, but have previously considered it* *C. We do not currently have a specific cyber security insurance policy and have not previously considered it*	A / B / C
Have you ever made any insurance claims for cyber security breaches under this insurance before?	Yes **/** No
In the last 12 months, approximately how much, if anything, do you think cyber security breaches or attacks have cost your organisation <u>in total</u> financially? ..... *This might include any of the following costs:* • *Staff stopped from carrying out day-to-day work* • *Loss of revenue or share value* • *Extra staff time to deal with the breach or attack, or to inform stakeholders* • *Any other repair or recovery costs* • *Lost or stolen assets* • *Fines from regulators or authorities, or associated legal costs* • *Reputational damage* • *Prevented provision of goods or services to customers* • *Discouragement from carrying out future business/charity activities* • *Goodwill compensation or discounts given to customers*	**£** **in last <u>12 months</u>**

Appendix B: Interviewer glossary

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

Term	Where featured	Definition
Cyber attack	Throughout	A cyber attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.
Cyber breach	Throughout	A security **breach** is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
Cyber security	Throughout	Cyber security includes any strategies, 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	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.
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 (now the Chartered Institute of Information Security)

NCSC	Q24 (DO NOT PROMPT)	National Cyber Security Centre – centre set up by government to issue guidance to businesses and charities, and also support organisations that have been breached
Hacking	Q53A, Q64A,	Hacking is unauthorised intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose.
Intellectual property	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, 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)
Password Policy	Q31	A standard definition of a strong password that all must use, e.g. minimum of 8 characters, lower and uppercase letters, at least one number and one special character etc.
Penetration testing	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
Personally-owned devices	Q8, Q32	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/charity-related activities
Pre-planned health checks vs. ad-hoc health checks	Q30	Health check activities might include things like staff surveys, security assessments or vulnerability scans. Pre-planned checks would be activities like this that are undertaken no a scheduled basis, e.g. annually. Ad-hoc checks will be the same kinds of activities but just undertaken as a one-off, e.g. in response to an attack.

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
Risk assessment covering cyber security risks	Q30	This is the process of identifying and controlling any cyber security threats to an organisation's data
Supply chain	Q45B	The network and sequence of processes between the organisation and its supplier to produce and distribute its goods or services to the end supplier
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

Consent

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

Yes
No CLOSE SURVEY

Business profile

Q1.DELETED POST-PILOT IN 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 IF BUSINESS (SAMPLE TYPE=1)
Q5X.TYPEX
Would you classify your organisation as … ?
READ OUT
INTERVIEWER NOTE: IF THEY HAVE A SOCIAL PURPOSE BUT STILL MAKE A PROFIT (E.G. PRIVATE PROVIDER OF HEALTH OR SOCIAL CARE) CODE AS CODE 1

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

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

SINGLE CODE
IF TYPEX CODES 1, 2 OR DK: Private sector
IF SAMPLE S_TYPE=2 OR TYPEX CODE 3: Charity
IF SAMPLE S_TYPE=3: State education institution

BASE [BUSINESS/CHARITY/EDUCATION] TEXT SUBSTITUTIONS ON TYPEXDUM (CHARITY IF TYPEXDUM CODE 2, EDUCATION IF TYPEXDUM CODE 3 ELSE BUSINESS). THIS IS THE DEFAULT SCRIPTING FOR ALL TEXT SUBSTITUTIONS FROM THIS POINT ONWARDS, UNLESS OTHERWISE SPECIFIED.

ASK ALL
Q4.SIZEA
Including yourself, how many [employees/employees, volunteers and trustees] work for your organisation across the UK as a whole?
ADD IF NECESSARY: [IF BUSINESS/EDUCATION: By that I mean both full-time and part-time employees on your payroll, as well as any working proprietors or owners. / IF CHARITY: By that I mean both full-time and part-time employees on your payroll, as well as people who regularly volunteer for your organisation.]
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE 2–500,000 (SOFT CHECK IF >99,999)

SINGLE CODE
Respondent is sole trader CLOSE SURVEY
Don't know

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

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

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

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

Q5A.SALESA DELETED PRE-PILOT IN CSBS 2020

Q5B.SALESB DELETED PRE-PILOT IN CSBS 2020

Q5Z.SALESDUM DELETED PRE-PILOT IN CSBS 2020

Q5C.YEARS DELETED POST-PILOT IN CSBS 2018

Q5D.CHARITYO DELETED PRE-PILOT IN CSBS 2019

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

MULTICODE
ROTATE LIST
Accounts or pages on social media sites (e.g. Facebook or Twitter)
ONLY SHOW IF BUSINESS/CHARITY: The ability for customers to order, book or pay for products or services online
ONLY SHOW IF CHARITY: The ability for people to donate online
ONLY SHOW IF CHARITY: The ability for your beneficiaries or service users to access services online
An online bank account your organisation [IF EDUCATION: pays/ELSE: or your clients pay] into
ONLY SHOW IF SAMPLE SICVAR=1: An industrial control system
ONLY SHOW IF BUSINESS/CHARITY: Personal information about your [IF BUSINESS: customers/IF CHARITY: beneficiaries, service users or donors] held electronically

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

Q7.CORE DELETED PRE-PILOT IN CSBS 2019

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 work-related activities, or not?

SINGLE CODE
Yes
No
Don't know

Perceived importance and preparedness

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

ASK ALL
Q9.PRIORITY
How high or low a priority is cyber security to your organisation's [INSERT STATEMENT]? Is it ...
READ OUT

a. [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management
b. **DELETED DURING FIELDWORK IN CSBS 2018**
c. **DELETED DURING FIELDWORK IN CSBS 2018**
    •

SINGLE CODE
REVERSE SCALE EXCEPT FOR LAST CODE
Very high
Fairly high
Fairly low
Very low
DO NOT READ OUT: Don't know

Q9A.HIGH DELETED POST-PILOT IN CSBS 2017

Q9B.RELPRIORITY DELETED POST-PILOT IN CSBS 2018

Q9C.OUTSOURCE DELETED PRE-PILOT IN CSBS 2020

Q10.LOW DELETED PRE-PILOT IN CSBS 2018

Q10A.ATTITUDES DELETED PRE-PILOT IN CSBS 2020

Q10B.LOWRISK REMOVED POST-PILOT IN CSBS 2017

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

SINGLE CODE
REVERSE SCALE EXCEPT FOR LAST 2 CODES
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

Spending

Q12.INVESTA DELETED PRE-PILOT IN CSBS 2020

Q13.INVESTB DELETED PRE-PILOT IN CSBS 2020

Q14.INVESTC DELETED PRE-PILOT IN CSBS 2020

Q15.INVESTD DELETED PRE-PILOT IN CSBS 2020

Q16.INVESTE DELETED PRE-PILOT IN CSBS 2020

Q17.INVESTF DELETED PRE-PILOT IN CSBS 2020

Q18.INVESTG DELETED PRE-PILOT IN CSBS 2020

Q19.ITA DELETED PRE-PILOT IN CSBS 2020

Q20.ITB DELETED PRE-PILOT IN CSBS 2020

Q21.REASON DELETED PRE-PILOT IN CSBS 2020

Q22.EVAL DELETED PRE-PILOT IN CSBS 2018

Q23.INSURE DELETED PRE-PILOT IN CSBS 2018

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

ASK ALL
Q23X.INSUREX
There are general insurance policies that provide cover for cyber security breaches or attacks, among other things. There are also specific insurance policies that are solely for this purpose. Which of the following best describes your situation?
READ OUT

SINGLE CODE
We have a specific cyber security insurance policy
We have cyber security cover as part of a broader insurance policy
We are not insured against cyber security breaches or attacks
DO NOT READ OUT: Don't know

ASK IF HAVE INSURANCE COVER (INSUREX CODES 1–2)
Q23Y.INSUREYES
Which of the following, if any, are provided under this insurance policy, as far as you know?
READ OUT

ASK AS A GRID
RANDOMISE LIST

a. Insurance against lost data
b. Insurance against lost earnings or profits
c. Help with reputation management following a breach
d. Help with incident response following a breach
e. Help with forensic analysis of breaches
f. Legal support following a breach

SINGLE CODE PER STATEMENT
Yes
No
DO NOT READ OUT: Don't know

Q23A.COVERAGE DELETED PRE-PILOT IN CSBS 2018

ASK IF HAVE INSURANCE (INSUREX CODE 1 OR 2)
Q23B.CLAIM
Have you ever made any insurance claims for cyber security breaches under this insurance before?

SINGLE CODE
Yes
No
Don't know

Q23C.NOINSURE DELETED PRE-PILOT IN CSBS 2020

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?")

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

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

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

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

External

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

SINGLE CODE
Nowhere
Don't know

Q24A.FINDINF DELETED POST-PILOT IN CSBS 2017

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

SINGLE CODE
REVERSE SCALE EXCEPT FOR LAST CODE
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

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

SINGLE CODE
Yes
No
Don't know

ASK ALL
Q24D.SCHEME
There are various Government schemes, information and guidance on cyber security. Which, if any, of the following have you heard of?
READ OUT

ASK AS A GRID
RANDOMISE LIST
a. The Cyber Essentials scheme
b. The 10 Steps to Cyber Security
c. IF MICRO OR SMALL BUSINESS (SIZEDUM CODES 1–2 AND TYPEXDUM CODE 1): Any Small Business Guides, such as the Small Business Guide to Cyber Security, or the Small Business Guide to Response and Recovery
d. IF MEDIUM OR LARGE (SIZEDUM CODES 3–4): The Cyber Security Board Toolkit
e. IF CHARITY (TYPEXDUM CODE 2): The Cyber Security Small Charity Guide

SINGLE CODE PER ROW
Yes
No
DO NOT READ OUT: Don't know

Training

Q25. DELETED POST-PILOT IN CSBS 2016

Q26.TRAIN DELETED PRE-PILOT IN CSBS 2020

Q26A.TRAINUSE DELETED POST-PILOT IN CSBS 2017

Q26B.TRAINWHO DELETED PRE-PILOT IN CSBS 2020

Q27.DELIVER DELETED POST-PILOT IN CSBS 2018

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. Again, just to reassure you, we are not looking for a "right" or "wrong" answer at any question.

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

MULTICODE
ROTATE LIST
[IF BUSINESS: Board members/IF CHARITY: Trustees/IF EDUCATION: A governor or senior manager] 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

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

Q29B.NOPOL DELETED PRE-PILOT IN CSBS 2020

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

MULTICODE
ROTATE LIST
CODE 4 MUST FOLLOW CODE 3
CODE 5 MUST FOLLOW CODE 6
Pre-planned internal audits or health checks that take place regularly
Ad-hoc internal audits or health checks, e.g. after breaches or news stories
An external audit
A risk assessment covering cyber security risks
Invested in threat intelligence
Used specific tools designed for security monitoring, such as Intrusion Detection Systems

SINGLE CODE
NOT PART OF ROTATION
DO NOT READ OUT: Don't know

DO NOT READ OUT: None of these

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

MULTICODE
ROTATE LIST
CODE 12 MUST FOLLOW CODE 11
Applying software updates when they are available
Up-to-date malware protection
Firewalls that cover your entire IT network, as well as individual devices
Restricting IT admin and access rights to specific users
Any monitoring of user activity
Specific rules for storing and moving personal data files securely
Security controls on company-owned devices (e.g. laptops)
Only allowing access via company-owned devices
Separate WiFi networks for staff and for visitors
Backing up data securely via a cloud service
Backing up data securely via other means
A password policy that ensures users set strong passwords

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

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

MULTICODE
ROTATE LIST
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

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

Q32A.FOLLOW DELETED POST-PILOT IN CSBS 2017

Q33.DOC DELETED PRE-PILOT IN CSBS 2019

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

SINGLE CODE
Within the last 6 months
6 to under 12 months ago
12 to under 24 months ago

24 months ago or earlier
DO NOT READ OUT: Don't know

Business standards

Q34.ISO DELETED DURING FIELDWORK IN CSBS 2018

Q35.IMPLEMA DELETED DURING FIELDWORK IN CSBS 2018

Q36.TENSTEPS DELETED PRE-PILOT IN CSBS 2020

Q37.ESSENT DELETED PRE-PILOT IN CSBS 2020

Q38.IMPLEMB DELETED PRE-PILOT IN CSBS 2020

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

Q44.SUPPLY DELETED PRE-PILOT FOR CSBS 2020

Q45.ADHERE DELETED PRE-PILOT FOR CSBS 2020

READ OUT TO ALL
The next question is about suppliers. This is not just security or IT suppliers. It includes any immediate suppliers that directly provide goods or services to your organisation. We also ask about your wider supply chain, i.e. your suppliers' suppliers.

Q45A.SUPPLYKNOW DELETED POST-PILOT IN CSBS 2020

ASK ALL
Q45B.SUPPLYRISK
Has your organisation carried out any work to formally review the following?
READ OUT

ASK AS A GRID
a. The potential cyber security risks presented by your immediate suppliers
b. The potential cyber security risks presented by your wider supply chain, i.e. your suppliers' suppliers

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

Q45C.SUPPLYCHK DELETED POST-PILOT IN CSBS 2020

Q45D.BARRIER DELETED POST-PILOT IN CSBS 2020

Cloud computing

Q46.CLOUD DELETED PRE-PILOT IN CSBS 2020

Q47. DELETED POST-PILOT IN CSBS 2016

Q48.CRITICAL DELETED POST-PILOT IN CSBS 2017

Q49.COMMER DELETED PRE-PILOT IN CSBS 2018

Q50.PERSON DELETED PRE-PILOT IN CSBS 2018

Q51.VALIDA DELETED POST-PILOT IN CSBS 2017

Q52.VALIDB DELETED POST-PILOT IN CSBS 2017

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

MULTICODE
ROTATE LIST
CODE 2 MUST FOLLOW CODE 1
CODE 7, 8 AND 9 TO STAY IN ORDER
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
ONLY SHOW IF EDUCATION: Unauthorised use of computers, networks or servers by students, even if accidental
Unauthorised use or hacking of computers, networks or servers by people [IF BUSINESS/CHARITY: outside your organisation/IF EDUCATION: other than staff or students]

MULTICODE
NOT PART OF ROTATION
Any other types of cyber security breaches or attacks

SINGLE CODE
NOT PART OF ROTATION
DO NOT READ OUT: Don't know
DO NOT READ OUT: None of these
DO NOT READ OUT: Refused

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

SINGLE CODE
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

Q55.NUMBA DELETED PRE-PILOT 2020

Q56.NUMBB DELETED PRE-PILOT 2020

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

MULTICODE
ROTATE LIST
CODE 4 MUST FOLLOW CODE 3
Software or systems were corrupted or damaged
Personal data (e.g. on [IF BUSINESS: customers or staff/IF CHARITY: beneficiaries, donors, volunteers or staff/IF EDUCATION: students 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
Your website or online services were taken down or made slower
Lost access to any third-party services you rely on

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

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

MULTICODE
ROTATE LIST
CODE 4 MUST FOLLOW CODE 3
Stopped staff from carrying out their day-to-day work
Loss of [IF BUSINESS: revenue or share value/ELSE: income]
Additional staff time to deal with the breach or attack, or to inform [IF BUSINESS: customers/IF CHARITY: beneficiaries/IF EDUCATION: students, parents] 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
ONLY SHOW IF BUSINESS/CHARITY: Prevented provision of goods or services to [IF BUSINESS: customers/IF CHARITY: beneficiaries or service users]
Discouraged you from carrying out a future business activity you were intending to do
Complaints from [IF BUSINESS: customers/IF CHARITY: beneficiaries or stakeholders/IF EDUCATION: students or parents]
ONLY SHOW IF BUSINESS/CHARITY: Goodwill compensation or discounts given to customers

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

Q58.MONITOR DELETED PRE-PILOT IN CSBS 2018

ASK IF ANY BREACHES OR ATTACKS (TYPE CODES 1–9)
Q11A.MICROSITE
We have a page on the Ipsos MORI website to help you answer the next questions and make the survey quicker. The webpage doesn't ask you to enter any information or download anything. Do you have a smartphone or computer to go to this webpage now, and have it open for the rest of the survey?

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

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

SINGLE CODE
Yes
No

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

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

SINGLE CODE
No cost incurred
Don't know
Refused

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

SINGLE CODE
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

SINGLE CODE
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

SINGLE CODE
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

Q61. DELETED POST-PILOT IN CSBS 2016

Q62. DELETED PRE-PILOT IN CSBS 2017

Q63.INCID DELETED PRE-PILOT 2020

ASK ALL
Q63A.INCIDCONTENT
Which of the following, if any, do you do, or have in place, for when you experience a cyber security incident?
READ OUT

MULTICODE
ROTATE LIST
Formally logging incidents
Written guidance on who to notify
Roles or responsibilities assigned to specific individuals during or after an incident
Attempting to identify the source of incident
An assessment of the scale and impact of the incident
Communications and public engagement plans

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

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

MULTICODE
ONLY SHOW CODES MENTIONED AT TYPE

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
ONLY SHOW IF EDUCATION: Unauthorised use of computers, networks or servers by students, even if accidental
Unauthorised use or hacking of computers, networks or servers by people [IF BUSINESS/CHARITY: outside your organisation/IF EDUCATION: other than staff or students]
Any other types of cyber security breaches or attacks

SINGLE CODE
DO NOT READ OUT: Don't know

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?")

MULTICODE
By accident
By antivirus/anti-malware software
Disruption to business/staff/users/service provision
From warning by government/law enforcement
Our breach/attack reported by the media
Similar incidents reported in the media
Reported/noticed by customer(s)/beneficiaries/service users/donors/students/customer complaints
Reported/noticed by staff/contractors/volunteers
Routine internal security monitoring
Other internal control activities not done routinely (e.g. reconciliations, audits etc)
Other WRITE IN

SINGLE CODE
None of these
Don't know

Q66.LENGTH DELETED PRE-PILOT IN CSBS 2020

Q67.FACTOR DELETED PRE-PILOT IN CSBS 2020

Q68.SOURCE DELETED PRE-PILOT IN CSBS 2020

Q69.INTENT DELETED PRE-PILOT IN CSBS 2020

Q70.CONTING DELETED PRE-PILOT IN CSBS 2019

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

SINGLE CODE
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

Q72.DEALA DELETED PRE-PILOT IN CSBS 2020

Q73.DEALB DELETED PRE-PILOT IN CSBS 2020

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 {IF BUSINESS: revenue/ELSE: income} if people could not access your services online.]

[IF USING MICROSITE (MICROSITE CODE 1): This includes the costs listed on the website under "direct results".]
PROBE FOR BEST ESTIMATE BEFORE CODING DK
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)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£99,999)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999)

SINGLE CODE
No direct result cost incurred
Don't know
Refused

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

SINGLE CODE

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

SINGLE CODE
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

SINGLE CODE
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

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 {IF BUSINESS: customers or stakeholders/IF CHARITY: beneficiaries, donors or stakeholders/IF EDUCATION: students, parents 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
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)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£99,999)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999)

SINGLE CODE

No recovery cost incurred
Don't know
Refused

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

SINGLE CODE
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

SINGLE CODE
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

SINGLE CODE
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

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:

- ONLY SHOW IF BUSINESS: loss of share value
- loss of {IF BUSINESS: investors/ELSE: donors} or funding
- long-term loss of {IF BUSINESS/CHARITY: customers (including potential new customers or business)/ IF EDUCATION: students (including potential new students)}

- 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
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)
IF MEDIUM (SIZEA 49<CODE<250 OR SIZEB CODE 3): (SOFT CHECK IF <£100 OR >£99,999)
IF LARGE (SIZEA 249<CODE OR [SIZEB CODES 4–5 OR DK]): (SOFT CHECK IF <£1,000 OR >£999,999)

SINGLE CODE
No long-term effects cost incurred
Don’t know
Refused

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

SINGLE CODE
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

SINGLE CODE
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

SINGLE CODE
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

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 [IF BUSINESS: directors or senior management/IF CHARITY: trustees/IF EDUCATION: governors or senior management] made aware of this breach, or not?

SINGLE CODE
Yes
No
Don't know

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?

SINGLE CODE
Yes
No
Don't know

ASK IF REPORTED (REPORTA CODE 1)
Q77.REPORTB
Who was this breach or attack reported to?
DO NOT READ OUT
PROBE FULLY ("ANYONE ELSE?")

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

SINGLE CODE
Don't know

Q77A.NOREPORT DELETED PRE-PILOT IN CSBS 2018

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?")

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

SINGLE CODE
Nothing done
Don't know

Q78B.NOACT DELETED POST-PILOT IN CSBS 2017

GDPR

Q78X.GDPRFINE DELETED PRE-PILOT IN CSBS 2020

Q78Y.GDPRREP DELETED PRE-PILOT IN CSBS 2020

Q78C.GDPRAWARE DELETED PRE-PILOT IN CSBS 2020

Q78D.GDPRCHANGE DELETED PRE-PILOT IN CSBS 2020

Q78E.GDPRCYBER DELETED PRE-PILOT IN CSBS 2020

Q78F.GDPRWHAT DELETED PRE-PILOT IN CSBS 2020

Q78G.GDPRSINCE DELETED POST-PILOT IN CSBS 2020

Q78H.GDPRCYBERA DELETED POST-PILOT IN CSBS 2020

Q78I.GDPRMORE DELETED POST-PILOT IN CSBS 2020

Q78J.GDPRCYBERB DELETED POST-PILOT IN CSBS 2020

Recontact and follow-up

ASK ALL
Q79.RECON
This survey is part of a wider programme of research. Would you be happy to take part in a more bespoke interview with Ipsos MORI in January or February 2020, to further explore some of the issues from this survey? ADD IF NECESSARY: the interviews would last no longer than 45 minutes and those taking part would be offered a £50 cheque or a donation to the charity of their choice.

SINGLE CODE
Yes
No

ASK ALL
Q80.REPORT
Would you like us to email you a copy of last year's report and a Government help card, with links to the latest official cyber security guidance for organisations like yours?

SINGLE CODE
Yes
No

ASK ALL
Q80a.PANELRECON
DCMS expects to carry out similar research within the next year. Your input is really important to help the Government to better understand and respond to organisations' cyber security needs, including ones like yours. Would you be happy for DCMS or their appointed contractor to contact you for your views on this topic again before the end of 2020?

SINGLE CODE
Yes
No

ASK IF WANT RECONTACT OR REPORT/HELPCARD (RECON CODE 1 OR REPORT CODE 1 OR PANELRECON CODE 1)
Q81.EMAIL
Can I please take an email address for you?

WRITE IN EMAIL IN VALIDATED FORMAT
Refused

SEND FOLLOW-UP EMAIL IF REPORT CODE 1

READ OUT TO ALL
Thank you for taking the time to participate in this study. Before you finish I need to inform you that you can access the privacy notice online at csbs.ipsos-mori.com. This explains the purposes for processing your personal data, as well as your rights under data protection regulations to:

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

CLOSE SURVEY

Appendix D: Help card offered to survey respondents

Government guidance for organisations on cyber security

Department for Digital, Culture, Media & Sport

Guidance for organisations just getting started

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

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

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

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

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

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

Guidance for established businesses and charities including micro and small organisations

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

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

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

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

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

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

Specific guidance for larger organisations

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

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

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

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

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

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

Appendix E: Topic guide

Prompts and probes	Timings and notes
Introduction	**2-3 minutes**
● Introduce yourself and Ipsos MORI – independent research organisation (i.e. independent of government) ● Commissioned through the government's National Cyber Security Programme, by the Department for Digital, Culture, Media & Sport (DCMS) ● Explain the research: we are speaking with businesses and charities to learn more about how they approach cyber security ● Confidentiality: all responses are confidential ● Length: around 45 minutes to 55 minutes ● Get permission to digitally record (and interview may be transcribed to help with our analysis) to help with notes and for anonymised quotes for report GDPR added consent (once recorder is on): ● Ipsos MORI's legal basis for processing is your consent to take part in this research. ● Your participation in this research is voluntary. ● You can withdraw consent for data to be used at any point before, during or after the interview. Can I check you are happy to proceed?	*The welcome helps to orientate the participant and gets them prepared to take part in the interview.* *Outlines the "rules" of the interview (including those we are required to tell them about under MRS guidelines). This includes GDPR-related consent.* *Make this very brief – we have already spoken to these individuals in the quantitative survey, so they should understand the background.*
Context	**2-3 minutes**
What's the main business/product/service of your organisation? Could you briefly describe your role? Just briefly for now, how do you think the topic of cyber security affects your organisation? What would you say are the top two or three risks an organisation like yours might face?	*This section provides context to follow up on later in the interview, in terms of who is in charge and what they see as the risks.* *Make this very brief.*
Changes to practices in medium term	**5 minutes**
How have things changed in how your organisation approaches cyber security since you have been in your role? ● How do the board or trustees view cyber security now? What's changed? ● What has changed to how you identify, manage and monitor potential risks related by cyber security? What protective measures are in place? ● How have you developed your rules and policies relating to cyber security? ● What has changed to how you react and manage an attempted breach should one occur? ● What other factors have caused change to your cyber security processes? PROBES on technological developments externally, cultural change towards cyber security both within and outside of organisation, upskilling within business, greater awareness of breaches and their impact.	*Have organisations gone from being reactive to breaches to proactive to stopping them?* *What changes have they made to their practices over the past five years?* *What planned changes do they have?*

● What planned changes do you have?	
Risk management and the supply chain	**12-15 minutes**
Who is responsible for managing the cyber security risks posed by your suppliers? What responsibility lies with the suppliers? What lies with your organisation? Why? ● Does this vary by type of supplier? If so, how and why? ● Have you spoken to their suppliers/senior managers about responsibility? Is it clearly defined? What did you discuss? ● What happens if they don't fulfil their responsibilities? What protection do you have? How do you know this is sufficient? ● If there is a breach within a supplier, who assumes responsibility? Does this vary by supplier? If so how and why? Is cyber security considered as a risk when you choose a supplier? How does it influence/factor into your choices? ● Is cyber risk built into contracts? What impact does this have on the cyber measures you take with suppliers? PROBES: impact of legal protection; greater knowledge/awareness ● To what extent does the relationship the supplier has with your wider IT systems influence this? Why? ● To what extent does the financial size of a supplier contract influence this? ● Is supplier risk considered in the procurement process/ by your commercial managers? How important is it? How important is the reputational risk? Is it considered? ● How aware are you of which suppliers have access to your IT systems? How does it affect how you manage cyber security risks? ● How aware are you of which of your suppliers are essential to the continuity of your organisation? How does it affect how you manage cyber security risks? How much of a priority is cyber security in your organisation generally? ● And do you give your suppliers' cyber security the same priority? Does the board in your company give priority to cyber security of your suppliers? ● How much have you thought specifically about supplier risks? Have you discussed it internally? What prompted these discussions? ● Have discussions considered supply chain as a whole, or your immediate suppliers or only selected strategic suppliers? What was the rationale behind this? ● Do suppliers prioritise cyber security and their supplier management as much as you? How do you know? Have you tried to find out? How do you gain assurance from your suppliers that they have robust cyber security? ● What are your typical approaches with suppliers when it comes to cyber security? ● Do you have approved suppliers?	*Are suppliers seen as a risk?* *How do organisations manage risk in the supply chain?* *What kind of standards are organisations enforcing on suppliers and how adequate do they feel these are?* *Could these standards be improved or made easier to implement?*

• What happens if someone wants to use a new supplier? What questions get asked? What processes are there? Does your organisation use standardised security contractual terms or negotiate these on a supplier by supplier basis? • PROBE • Different for different suppliers? How do they distinguish different types of suppliers? • What's documented/written into policies/contracts? • When do any checks take place? At start of supplier contracts, throughout, at regular intervals etc.? What's the rationale for this? • How did you decide on this process? What's it based on? How do you know it's good enough? What challenges do you face when dealing with cyber security risks from suppliers? • What about when monitoring suppliers? PROBE time, resources, skills/knowledge, maintaining good supplier relationships, burden on supplier, competing priorities • What would support you to do this better? • What guidance/information needs do you require, if any? • Do you monitor the risks posed by the wider supply chain? If so, how and why? If not, why?	

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

SECTION ONLY RELEVANT IF FLAGGED BROWN IN THE SAMPLE (PRIORITY #1): Insurance	**10-12 minutes**
In the survey, you mentioned that you have a cyber insurance policy. Do you have a standalone policy or is it included in some other form of cover (i.e. property insurance)? If a standalone policy, what was the motivation behind getting this? Was this the first time you have bought cyber insurance? If so, what pushed you to do so this time? (PROBES ON BROKER; ADVERTISING CAMPAIGN) How did you choose your policy? Did you compare multiple different policies? What were your main concerns when buying cyber insurance? PROBES ON BREADTH OF COVERAGE, LIKELIHOOD OF GETTING A PAYOUT, LIKELIHOOD OF SUFFERING AN ATTACK. What do you think you gain from having cyber insurance? PROBES ON HAVING ACCESS TO BREACH ANALYSIS; SOFTENED REPUTATIONAL DAMAGE; POST BREACH SUPPORT	*What are the more and less important drivers behind having cyber insurance?* *Are there any positive behavioural impacts from having cyber insurance? Does it mandate or encourage better cyber security?* *How would you expect a claims process to pan out and would it be worth it?*

Does your insurance policy require you to meet certain cyber security standards or requirements? ● Did you have to make changes to meet these standards/requirements or was your existing cyber risk management approach sufficient? ● Did purchasing cyber insurance have any other impacts on your organisation's approach to cyber security? PROBES ON IF BUYING CYBER INSURANCE MADE THEM REASSESS THEIR OVERALL CYBER RISK AND MADE ADDITIONAL CHANGES NOT REQUIRED BY THE INSURER. What kinds of breaches/cyber risks would you expect to make a claim for under this insurance? PROBES ON RANSOMWARE, VIRUSES, SPYWARE, MALWARE, WEBSITE BEING TAKEN DOWN, HACKING OF BANK ACCOUNTS, IMPERSONATION, ANAUTHORISED USED OF COMPUTERS/NETWORKS ● What would be severe enough to make a claim? ● How easy do you think it would it be to make a claim? What would be the challenges? How easy would it be to compile the right information?	
SECTION ONLY RELEVANT IF FLAGGED BLUE IN THE SAMPLE (PRIORITY #1): Those without insurance	**2-3 minutes**
You mentioned in the survey that you do not have any cyber insurance policy. Why do you currently feel you do not need cyber insurance? How does this impact your organisation's risk to a cyber breach? Why? Have you considered getting cyber insurance before? Why/why not? ● Would this be a specific policy or as part of a wider more general insurance policy? Why? ● What would it take to consider cyber insurance?	*Why do businesses not have cyber insurance? Would they ever consider it?*
SECTION ONLY RELEVANT IF FLAGGED GREEN IN THE SAMPLE (PRIORITY #2): Audits	**7-8 minutes**
You mentioned in the survey that you undertake audits or health checks to identify cyber security risks to your organisation. Are you able to briefly explain to me what an audit or health check involves? ● Where does your audit process come from? How did you draw it up in the first place? ● How long has it been in place? Has it evolved over time? What were the reasons behind any changes? ● Who carries out the audit? What team are they in (HR, IT, other)? What skills/qualifications do they have? ● What's the main purpose of the audits? Who is it reported to? What do they do with this information? PROBE internal reporting, external	*What does an audit involve? Why do they do them? How often do they undertake audits? Who gets involved? What are the differences between internal and external audits?*

reporting (e.g. annual reports), board involvement, insurance companies, compliance, external bodies • What's the frequency of audits? What's the rationale for this? IF AD HOC: Why was it just a one-off? Would there be value in repeating it more regularly? Why hasn't this been done? • Has anything ever been changed or picked up off the back of audits? PROBE FOR DETAILS/SPECIFICS IF ONLY ONE OF INTERNAL OR EXTERNAL: What make you do audits internally rather external audits (or vice versa)? • PROBE Resources, skills, time, compliance needs, other reasons What do you do after the audit? • What changes or improvements have you made? • What's the minimum standard you would like to prove you have achieved through the audit? Why was it introduced? Who decides this? Do you feel senior management understands this?	
SECTION ONLY RELEVANT IF FLAGGED ORANGE IN THE SAMPLE (PRIORITY #3): Not acting on breaches	**5-7 minutes**
You mentioned in the survey that you had a disruptive breach last year (RAISE DETAILS FROM SURVEY TO PROMPT). Tell me a bit about the circumstances and what happened. In the survey, you said you did nothing specific in response to the breach. Just checking, did you take any actions to help you recover? Did you take any actions to prevent future breaches? What are your reasons for not taking further action? PROBE: Lack of time, resources, skills/knowledge, nothing we could have done, security already good enough, lack of magnitude, was a one-off etc. IF HAVE INSURANCE: Why did you not make a claim under your cyber insurance policy? How avoidable was this breach? What do you think you could have done? What would have made a difference? Could this kind of breach happen again? How likely is it? How much was this discussed at the time of the breach? How involved has the board been? What would cause you to take action? PROBE ON level of incident, type of incident, disruption to operations, potential costs, reputation management. Why is this?	*Why are organisations not taking action on certain breaches?* *What kind of breach requires action? What kind does not?*

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

Reporting breaches	**5-7 minutes**
You told us in the survey that you [did] [did not] report a breach when one occurred. Can you explain why? FOR THOSE THAT REPORTED A BREACH: You said in the survey that you reported a breach you had last year to someone outside your organisation. Can you tell me a bit about this? ● What made you decide to report this? ● How did you know who to report it to? ● What was the experience of reporting a breach like? PROBE burden, internal discussions/concerns ● When I talk about reporting a cyber security breach, what does that mean to you? FOR THOSE THAT DID NOT REPORT A BREACH: Why did you not report the breach externally? PROBES lack of confidence in authorities; did not think anything could be done; fear of reputational damage What kinds of breaches would you report? What kinds wouldn't you report? What are the key differences? PROBES severity of breach, frequency, criminality ● Are there any that have to be reported? ● Who would you report it to? Does it differ for different kinds of breaches PROBES – Action Fraud, Police etc. ● IF NOT Action Fraud: Before taking part in the survey, were you aware of Action Fraud? ● What are the reasons for reporting breaches? What do you think the most important reasons are? What do you/others get from it? PROBES benefits to organisation, benefits to society ● Are there any risks with reporting breaches? Any concerns you might have? ● What might encourage you to report breaches in the future?	*What motivates organisations to report breaches? Why are they not reporting breaches? Who do they report breaches to? What support do they need?*
Information sources and government guidance	**10 minutes**
We sent you some links to government information and guidance before this interview and asked you to take a look. Which ones have you looked at? ROTATE AS RELEVANT: Charities guide; Small business guide; 10 Steps; Board toolkit; Cyber Aware; NCSC website ● What did you think of these? ● How relevant are they for your organisation? ● What do you like about them? What works well? ● What works less well? What could be improved? ● How much do these things address your needs? What is missing? What questions/support needs do you still have? ● What other kinds of information/guidance would be useful? ● Have you seen anything like this before? Where was this?	*How aware are people of key messaging in government sources of info? Has this changed over time? What do they think of the 10 steps guidance?*

If you saw information/guidance like this, would it prompt you to do anything differently/make any changes? Would it prompt any internal discussions/checks? Have you used any guidance in the past? If so, how helpful has it been in implementing any changes/ increasing awareness in the organisation?	
Wrap up	**2-3 minutes**
Overall, what do you think is the one thing I should take away from the discussion today? IF NOT ON PROFILE INFORMATION, COLLECT INCENTIVE DETAILS (£50 CHEQUE, BANK TRANSFER OR CHARITY DONATION) THANK AND CLOSE	*Wrap up interview.*

Appendix F: Further information

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

   - Harry Williams, Ipsos MORI
   - Jayesh Navin Shah, Ipsos MORI
   - Lydia Clark, Ipsos MORI

2. The Cyber Security Breaches Survey was first published in 2017 as a research report, and became an Official Statistic in 2018. The previous reports can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey. This includes the full report, infographics and the technical and methodological information for each year. The next version of the Cyber Security Breaches Survey is expected to be published in 2021.

3. The responsible DCMS analyst for this release is Emma Johns. The responsible statistician is Rishi Vaidya. For enquiries on this release relating to official statistics, please contact Rishi on 020 7211 2320 or evidence@culture.gov.uk.

4. For general enquiries contact:

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

   Telephone: 020 7211 6000

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

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

7. This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms.

Department for Digital, Culture, Media & Sport

4th Floor
100 Parliament Street
London
SW1A 2BQ