Department for Digital, Culture, Media & Sport

Ipsos MORI

Cyber Security Breaches Survey 2021

Technical Annex

This Technical Annex provides the technical details of the Cyber Security Breaches Survey 2021. It covers the quantitative survey (fieldwork carried out in winter 2020 and 2021) and qualitative element (carried out in early 2021), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

The annex supplements a main Statistical Release and infographic summaries published by the Department for Digital, Culture, Media and Sport (DCMS), covering the this year's results for businesses and charities.

There is another Education Institutions Findings Annex, available on the same GOV.UK page, that covers the findings for schools, colleges and universities.

The Cyber Security Breaches Survey is a quantitative and qualitative study of UK businesses, charities and education institutions. 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 2020/21 and the qualitative element in early 2021.

Responsible analyst:

Emma Johns
07990602870

Statistical enquiries:

evidence@dcms.gov.uk
@DCMSinsight

General enquiries:

enquiries@dcms.gov.uk

Media enquiries:

020 7211 2210

Contents

Chapter 1: Overview

1.1 Summary of methodology

As in previous years, there were two strands to the Cyber Security Breaches Survey 2021:

- We undertook a random probability telephone survey of 1,419 UK businesses, 487 UK registered charities and 378 education institutions from 12 October 2020 to 22 January 2021. The data for businesses and charities have been weighted to be statistically representative of these two populations.
- We carried out 32 in-depth interviews in January 2021, to gain further qualitative insights from some of the organisations that answered the survey.

Sole traders and public-sector organisations were outside the scope of the survey. In addition, businesses with no IT capacity or online presence were deemed ineligible, which led to a small number of specific sectors (agriculture, forestry and fishing) being excluded. These exclusions are consistent with previous years, and the survey is considered comparable across years.

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 2021 survey shares the same strengths as previous surveys in the series:

- the use of random probability sampling and interviewing 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, giving respondents flexibility in how they can answer (e.g. allowing numeric and banded £ amounts), and sending them a follow-up online survey to validate answers given in telephone interviews
- a consideration of the cost of cyber security breaches beyond the immediate direct costs (i.e. explicitly asking respondents to consider longer-term direct costs, staff time costs, as well as other indirect costs, while giving a description of what might be included within each of these cost categories) – this approach has been strengthened this year, which we cover in Section 2.1.

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. As we allude to in the main Statistical Release, this could be a more significant limitation this year, since organisations may have had less oversight of their staff during the COVID-19 pandemic.
- 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). In the improvements made this year to the cost questions, we consciously opted to not to ask about certain long-term indirect costs, as it was unrealistic to collect accurate figures for these areas in a single survey. This is expanded on in Section 2.1.

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 surveys since 2020.

The 2021 survey is also methodologically consistent with previous years. However, there are some significant changes for readers to be aware of:

- We increased the sample sizes for businesses (from 1,348 last year to 1,419 this year), charities (from 337 to 487) and state education institutions (from 287 to 378). The biggest impacts of these increases are on the charities and education institutions samples, where the higher sample sizes allow for more granular analysis. We are able to analyse results by income band for charities, and to more robustly split out the results for primary schools, secondary schools and colleges.
- The scope of the school and college samples were expanded to include institutions in Wales, Scotland and Northern Ireland, as well as England.
- We substantially changed the way we collect data on the costs of breaches in the survey, as part of a reflection on findings from a separate 2020 DCMS research study on the full cost of cyber security breaches. These changes mean cannot make direct comparisons between this year's data and previous years. We can, however, still comment on whether the broad patterns in the data are consistent with previous years, for example the differences between smaller and larger businesses, as well as charities.
- More broadly, we increased the average questionnaire lengths from c.17 minutes in 2020 to c.20 minutes this year. This reflected space required for new topics related to DCMS's policy objectives (e.g. new questions related to COVID-19 and managing supplier risks). The thematic list of questionnaire additions is in Section 2.1.

1.4 Comparability to the pre-2016 Information Security Breaches Surveys

From 2012 to 2015, the government commissioned and published annual Information Security Breaches Surveys.[1] While these surveys covered similar topics to the Cyber Security Breaches Survey series, they employed a radically different methodology, with a self-selecting online sample weighted more towards large businesses. Moreover, the question wording and order is different for both sets of surveys. This means that comparisons between surveys from both series are not possible.

[1] 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.

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 briefing materials). DCMS had final approval of the questionnaire. Development for this year's survey took place over three stages from July to September 2020:

- stakeholder engagement, including a virtual workshop with industry and government representatives
- cognitive testing interviews with 10 organisations (businesses, charities and schools)
- a pilot survey, consisting of 24 interviews (10 businesses, 12 charities and 2 schools).

A full list of all questionnaire amends since 2020 is included at the end of this section.

Stakeholder engagement and initial questionnaire review (including academic input)

This year, Steven Furnell, Professor of Cyber Security from the University of Nottingham, was involved as an academic consultant in the survey development. As part of the initial questionnaire review, Professor Furnell engaged with academic colleagues from various UK universities in July and August 2020 to seek feedback on the previous questionnaire and suggested changes. He also carried out his own review of the questionnaire to see how well it mapped to the latest NCSC guidance on cyber security for organisations.

Ipsos MORI held a virtual workshop with a government and industry stakeholders in August 2020, to collect feedback on past studies and discuss new areas of interest for the 2021 study. These included the Association of British Insurers (ABI), the British Insurance Brokers' Association (BIBA), the Confederation of British Industry (CBI), TechUK and the Institute of Chartered Accountants in England and Wales (ICAEW). Government stakeholders included the Home Office, the Treasury and the National Cyber Security Centre (NCSC). Professor Furnell presented the findings of his review at this workshop as well.

Outside of this workshop, we also had separate meetings with the NCSC, facilitated by the DCMS project team, to discuss how to best approach and promote the survey with education institutions.

Based on these discussions, the feedback from stakeholders, and their own internal thinking, DCMS agreed the following new questions or question statements to add to the questionnaire:

- respondent job titles (TITLE), to give a sense of the seniority of those dealing with cyber security and their placement within organisations
- the presence of unsupported versions of Windows (at ONLINE)
- the presence of new technologies and IT solutions like smart devices (at ONLINE and POLICY) and Software as a Service (also at POLICY)
- questions on COVID-19, including whether cyber security prioritisation had changed as a result of the pandemic (COVPRI), the presence of Virtual Private Networks (at RULES), capturing awareness of NCSC guidance related to home working, video conferencing and moving business online (at SCHEME)
- the actions organisations had taken as a result of seeing government guidance (GOVTACT) – this also led to a refresh of the unprompted code list at PREVENT (actions taken after breaches) to align both these questions
- accreditations that organisations adhered to (COMPLY)
- new questions on phishing, including whether organisations do mock phishing exercises (at IDENT) and whether staff have a process to follow for phishing emails (at RULES)
- whether organisations do penetration testing (at IDENT)

- whether organisations had undertaken cyber security training or awareness raising (TRAINED) – the survey does not explore cyber security training in depth because there is a separate annual DCMS survey on this topic, but this question was necessary to better map the questionnaire to the 10 Steps to Cyber Security government guidance
- barriers organisations faced when reviewing supply chain cyber risks (BARRIER).

We added categories to TYPE to more comprehensively cover all types of cyber security breaches (including video conferencing breaches and hacking of logins or websites). Related to this, we also added to OUTCOMES to capture cases where hacked accounts were used for illicit purposes.

The following questions were also significantly amended so cannot be compared to previous years:

- the category relating to patching (at RULES) – this is now a substantially more stringent than before, asking organisations if they have a policy to apply security updates within 14 days of their release, rather than whether they apply security updates in general
- the presence of business continuity plans – now specifically asking if these plans cover cyber security (at MANAGE)
- questions capturing internal and external audits now explicitly refer to a cyber security vulnerability audit, to avoid confusion with non-cyber-related financial audits (at IDENT).

The following questions were removed, partly to make space for the additions:

- how useful government guidance was considered to be (GOVTINF)
- how organisations had originally identified their breaches (IDENTB)
- questions that were considered for inclusion but removed after the pilot due to lack of space, including why COVID-19 had changed the importance of cyber security, and a more in-depth exploration of the specific breaches that had caused negative outcomes or impacts on organisations.

Finally, this year, we made significant changes to the wording and ordering of the cost of breaches questions in the survey, in order to improve the accuracy of the cost data. These improvements included:

- redesigning the granular cost questions to follow the cost mapping laid out in a separate 2020 DCMS research study on the full cost of cyber security breaches
- moving the order of the overarching cost question (COST) to be after these more granular ones, to allow a better consideration of overall costs.

The 2020 DCMS study on costs advocated splitting cost categories into short, medium and long-term costs, as well as direct cost (i.e. where there was a direct cash transfer, like a fraudulent invoice payment or money stolen) and indirect cost (e.g. staff time or other spending that came about as a result of the breach) for each of these timeframes. It was not feasible to have this level of granularity in this survey. Moreover, we considered it unrealistic to collect the long-term indirect costs, as we expected that many of these answers would be speculative. Therefore, our questions focus on collecting:

- short-term direct costs (i.e. those faced during the breach)
- longer-term direct costs (those faced in the aftermath of a breach)
- staff time costs
- other short and medium-term indirect costs.

Cognitive testing

The Ipsos MORI research team carried out 10 cognitive testing interviews with businesses, charities and schools to test comprehension of new or changed questions for 2021.

We recruited all participants by telephone. There were multiple sample sources. In the first instance, we looked to recruit organisations that had taken part in last year's survey and had given permission for recontact. As a secondary sample source, we also purchased business sample from the Dun & Bradstreet business directory, took a random selection of charities from the charity regulator and schools from the Get Information About Schools database. We applied recruitment quotas and offered £50 incentive[2] to ensure participation from different-sized organisations across the country, from a range of sectors or charitable areas.

After this stage, the questionnaire only required minor tweaks. We tweaked wording for the categories at questions like ONLINE, SCHEME, IDENT, POLICY and TYPE to ensure they were as concise as possible and fully understood by respondents.

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 interviewer briefing materials
- 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 28 September and 8 October 2020. Again, we applied quotas to ensure the pilot covered different-sized businesses from a 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 and further education samples, as the populations are so small (making the available sample precious). We carried out 24 interviews, breaking down as:

- 10 businesses
- 12 charities
- 2 schools.

The pilot sample came from the same sample frames used for the main stage survey (see next section). In total, we randomly selected 480 business leads, 400 charity leads and 240 schools.

The questionnaire length for the pilot was 22 minutes, which was above target for the main stage. Following feedback from the pilot survey and having assessed the interview length during the first 150 interviews during mainstage fieldwork, we made some changes to the questionnaire:

- amending TITLE to exclude team or department
- deleting various questions (those noted above that were added in the development phase, as well as questions from last year, including INSUREYES and MICROSITE).

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

This year, the pilot was also used as a soft launch of the main fieldwork. We used the same sample frames for the main stage. The sample selection and interviewing process for the pilot was random. Moreover, there were no substantial post-pilot changes other than cuts to the questionnaire. Therefore, the 24 pilot interviews were counted as part of the final data, whereas in previous years, these have not been merged.

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

2.2 Survey microsite and GOV.UK page

As in previous years, a publicly accessible Ipsos MORI microsite (still active as of April 2021) and a similar GOV.UK page were again used to provide reassurance that the survey was legitimate and provide more information before respondents agreed to take part.

Interviewers could refer to both pages at the start of the telephone call, while the reassurance emails sent out from the CATI script (e.g. to organisations that wanted more information) included a link to the GOV.UK page.

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, i.e. private companies or non-profit organisations[3] with more than one person on the payroll.

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.

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. This exclusion is reviewed annually by DCMS.

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: https://register-of-charities.charitycommission.gov.uk/register/full-register-download
- the Office of the Scottish Charity Regulator database: https://www.oscr.org.uk/about-charities/search-the-register/charity-register-download

[3] These are organisations that work for a social purpose, but are not registered as charities, so not regulated by the UK's charity regulators.

- 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. DCMS was granted full access to the non-public OSCR database, including telephone numbers, meaning we could sample from the full list of Scotland-based charities, rather than just those for which we were able to find telephone numbers.

The Charity Commission in Northern Ireland does not yet have a comprehensive list of established charities, but has been registering charities and building its list over the past few years. Alternative sample frames for Northern Ireland, such as the Experian and Dun & Bradstreet business directories (which also include charities) have been considered in previous years, and ruled out, because they do not contain essential information on charity income for sampling, and cannot guarantee up-to-date charity information.

Therefore, while the Charity Commission in Northern Ireland database was the best sample frame for this survey, it cannot be considered as a truly random sample of Northern Ireland charities at present. This year, there were 6,190 registered charities on the Northern Ireland database, compared to 6,118 in the 2020 survey and 6,078 in the 2019 survey.

Education institutions population and sample frame

The education institutions sample frame came from the sources:

- All institutions in England: Get Information About Schools
- Schools in Scotland: Scottish Government School Contact details
- Further education colleges in Scotland: Colleges Scotland directory
- Schools in Wales: Welsh Government Address list of schools
- Further education colleges in Wales: Colleges Wales directory
- Schools in Northern Ireland: Northern Ireland Department of Education database
- Further education colleges in Northern Ireland: NI Direct FE College directory
- online lists of all UK universities, e.g. the Universities UK website, cross-referenced against the comprehensive list of Recognised Bodies on GOV.UK (which also includes, for example, degree-awarding arts institutes).

Given the significant differences in size and management approaches between different types of education institutions, we split the sample frame into four independent groups:

- 20,823 primary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 5 to 11)
- 3,976 secondary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 11+)
- 309 further education colleges
- 175 universities.

Business sample selection

In total, 89,372 businesses were selected from the IDBR for the 2021 survey. This is higher than the 79,031 selected in 2020 and 77,432 selected in 2019 and much higher than the 53,783 businesses selected for the 2018 survey, and the 27,948 selected in the 2017 survey.

We chose to increase the number to mitigate against the risk of varying sample quality experienced in recent years (in terms of telephone coverage and usable leads), as well as the anticipated difficulty in reaching businesses during the COVID-19 pandemic. We wanted to ensure that there was enough reserve sample to meet the size-by-sector survey targets. For example, in previous years, we had used up all reserve sample in the largest size band.

Ultimately, the 2021 sample quality and telephone coverage turned out to be similar to the 2020 sample, 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 2020, published by the Department for Business, Energy and Industrial Strategy (BEIS). 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 2020 report. The boosted sectors included:

- financial and insurance
- health, social work or social care
- information and communications
- manufacturing.

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

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

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

SIC 2007 letter[4]	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)	2,549	371	144	473	3,537
F	Construction	10953	54	176	266	11,449
G	Retail or wholesale (including vehicle sales and repairs)	4,596	185	484	1220	6,485
H	Transport or storage	4,057	38	170	314	4,579
I	Food or hospitality	5,344	244	311	463	6,362
J	Information or communications	16,015	363	174	425	16,977
K	Finance or insurance	1,313	402	176	391	2,282
L, N	Administration or real estate	9,343	129	418	975	10,865
M	Professional, scientific or technical	12,974	100	348	753	14,176
P	Education	883	28	46	50	1,007
Q	Health, social care or social work	7,438	309	93	224	8,064

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

SIC 2007 letter[4]	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
R, S	Entertainment, service or membership organisations	3,154	69	106	260	3,589
	Total	**78,619**	**2,292**	**2,646**	**5,814**	**89,372**

Charity and education institution sample selection

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.

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 state education institution databases 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:

- 77,878 of the 89,372 original IDBR records had either no telephone number or an invalid telephone number (i.e. the number was either in an incorrect format, too long, too short, had an invalid string, or was a number which would charge the respondent when called)
- 4,418 of the 199,742 charities had no valid telephone numbers
- 163 of the 25,283 education institutions had no valid telephone numbers.

We carried out telephone tracing (matching the sample frame data to the Dun & Bradstreet database and to any publicly available data sourced from LinkedIn) to fill in the gaps where possible. The sample was also cleaned to remove any duplicate telephone numbers.

At the same time as this survey, Ipsos MORI was also carrying out another business survey with a potentially overlapping sample – the DCMS cyber skills labour market survey. We therefore flagged overlapping sample leads across surveys, so telephone interviewers could avoid contacting the same organisations in quick succession for both surveys, and minimise the burden on respondents.

Following telephone tracing and cleaning, the usable business sample amounted to:

- 29,074 IDBR records
- 169,476 charities (with exclusions mainly due to the high prevalence of duplicate numbers in this sample frame)
- 18,307 education institution.

Given the particularly low size of the college and university population groups, and the available large business sample, we also carried out extensive manual sample improvement for these groups. This involved looking up relevant contact names and numbers online and on LinkedIn (on publicly available pages) wherever possible. This was done in two stages – firstly, ahead of

main fieldwork, and again at the halfway point in fieldwork (when more of the sample was found to have unusable numbers).

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)	922	309	132	425	1,788
		36%	83%	92%	90%	51%
F	Construction	3,327	38	160	236	3,761
		30%	70%	91%	89%	33%
G	Retail or wholesale (including vehicle sales and repairs)	1,436	140	435	1,079	3,090
		31%	76%	90%	88%	48%
H	Transport or storage	751	29	163	283	1,226
		19%	76%	96%	90%	27%
I	Food or hospitality	1,201	107	254	399	1,961
		22%	44%	82%	86%	31%
J	Information or communications	3,227	206	146	357	3,936
		20%	57%	84%	84%	23%
K	Finance or insurance	723	310	157	344	1,534
		55%	77%	89%	88%	67%
L, N	Administration or real estate	2,159	72	348	858	3,437
		23%	56%	83%	88%	32%
M	Professional, scientific or technical	3,354	64	312	649	4,379
		26%	64%	90%	86%	31%
P	Education	244	17	36	44	341
		28%	61%	78%	88%	34%
Q	Health, social care or social work	1,833	192	85	199	2,309
		25%	62%	91%	89%	29%
R, S	Entertainment, service or membership organisations	941	42	97	232	1,312
		30%	61%	92%	89%	37%
	Total	**20,118**	**1,526**	**2,325**	**5,105**	**29,074**

SIC 2007 letter	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
		26%	**67%**	**88%**	**88%**	**33%**

Sample batches

For businesses and charities, the usable sample for the main stage survey was randomly allocated into separate batches. The first business batch, excluding pilot sample, had 6,644 records proportionately selected to incorporate sample targets by sector band, disproportionately selected to include more medium and large businesses owing to the expected difficulty in contacting these businesses and response rates by sector and size band from the 2020 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. Similarly, the first charity batch had 1,471 records selected to match the disproportionate targets and expected response rates by income band.

Over the course of fieldwork, we used (including for the pilot):

- 17,949 IDBR records
- 2,502 charity records.

For primary and secondary schools, we selected a simple random sample of each group. This amounted to:

- 280 primary schools in the first batch and 400 in total across all batches (including the pilot sample)
- 420 secondary schools in the first batch and 690 in total.

For businesses, charities and schools, subsequent batches (after the initial batch) were drawn up and released as and when live sample was exhausted.

The colleges and higher education institutions sample was released in full at the start of fieldwork (i.e. we carried out a census of these groups, only excluding a handful of records where there was no valid telephone number). This amounted to:

- 305 further education colleges
- 173 higher education institutions.

Across all sample groups, six batches of sample were released throughout fieldwork. We aimed to maximise the response rate by fully exhausting the existing sample batches before releasing additional records. This aim was balanced against the need to meet interview targets, particularly for boosted sample groups (without setting specific interview quotas).

2.4 Fieldwork

Ipsos MORI carried out all main stage fieldwork was from 12 October 2010 to 22 January 2021 using a Computer-Assisted Telephone Interviewing (CATI) script. This was an overall fieldwork period when compared with the 2020 survey (13 weeks[5], vs. 10 weeks last year). This reflected the considerable challenges faced this year in terms of interviewing during the COVID-19 pandemic. We discuss this further at the end of Section 2.5.

In total, we completed interviews with:

[5] This excludes the two weeks around the Christmas and New Year bank holidays, during which there was minimal fieldwork conducted.

- 1,419 businesses
- 487 charities
- 135 primary schools
- 158 secondary schools
- 57 further education colleges
- 28 higher education institutions.

The average interview length was c.20 minutes for all groups.

Fieldwork preparation

Prior to fieldwork, the Ipsos MORI research team briefed the telephone interviewing team in a video call. They also received:

- written briefing materials about all aspects of the survey
- a copy of the questionnaire and other survey instruments.

Screening of respondents

Interviewers screened all sampled organisations at the beginning of the call 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, with the list reviewed by the Ipsos MORI research team for inconsistencies
- 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.

At this point, interviewers specifically asked for the senior individual with the most responsibility for cyber security in the organisation. The interviewer briefing materials included written guidance on likely job roles and job titles for these individuals, which would differ based on the type and size of the organisation.

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 interviewing 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. This year, all leads ended up being 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.
- Ipsos MORI set up an email inbox and free (0800) phone number for respondents to be able to contact to set up appointments or, in the case of the phone number, take part there and then in interviews. Where we had email addresses on the sample for organisations, we also sent four warm-up and reminder emails across the course of fieldwork to let businesses know that an Ipsos MORI interviewer would attempt to call them. These were generic email addresses, rather than ones for specific individuals in the business.
- The survey had its own web page on GOV.UK and the Ipsos MORI microsite, 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 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 email respondents a copy of last year's infographic summaries, 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 B.
- Specifically, to encourage participation from colleges and universities, DCMS and Ipsos MORI jointly worked with the NCSC and Jisc (a membership organisation of individuals in digital roles within the further and higher education sectors), asking them to promote the survey. This included emailing members, making use of a promotional PowerPoint deck that Ipsos MORI drafted with the survey details.

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.

Online follow-up survey to revalidate cost data

As part of a redesigned approach to collecting cost data this year, we added a new online follow-up survey. Respondents who gave permission at the end of the telephone interview were sent a unique online link allowing them to recheck the answers they had given to the four cost of breaches questions in the survey, and change them if they wanted to. The online version of these questions had the same question wording, but the online format allowed for a clearer presentation, highlighting all the types of costs we wanted respondents to consider in their answer. Respondents were also encouraged with this follow-up survey to validate their answers with others in their organisation (e.g. finance or legal colleagues).

As well as the original invite, we sent two reminder emails during the main fieldwork period to those that had offered to fill in the survey but had not completed it.

A total of 772 respondents were sent this follow-up survey (i.e. they gave their consent), out of the total 1,041 respondents that were eligible (i.e. had identified breaches or attacks in the telephone survey). Of these, 170 completed the follow-up, representing a response rate of 22% for this online element. Only 18 respondents changed any of their answers, and this was usually just one of their answers across the five cost questions. This helps to provide a high level of confidence in the cost estimates reported in the main Statistical Release.

2.5 Fieldwork outcomes and response rate

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

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

Outcome	Businesses	Charities
Total sample loaded	17,947	2,700
Completed interviews	1,419	487
Incomplete interviews	81	30
Ineligible leads – established during screener[7]	294	10
Ineligible leads – established pre-screener	86	6
Refusals[8]	3,894	536
Unusable leads with working numbers[9]	4,443	555
Unusable numbers[10]	2,249	160
Working numbers with unknown eligibility[11]	5,481	718
Expected eligibility of screened respondents[12]	84%	98%

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

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

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

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

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

[11] This includes sample that had a working telephone number but where the respondent was unreachable or unavailable for an interview during the fieldwork period, so eligibility could not be assessed.

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

Outcome	Businesses	Charities
Expected eligibility of working numbers[13]	47%	64%
Unadjusted response rate	8%	19%
Adjusted response rate	19%	32%
Cooperation rate[14]	28%	49%

The fieldwork outcomes for state education institutions are shown in Table 2.4.

Table 2.4: Fieldwork outcomes and response rate calculations for state education institutions

Outcome	Primary schools	Secondary schools	Colleges	Higher education
Total sample loaded	400	690	305	173
Completed interviews	135	158	57	28
Incomplete interviews	6	4	1	0
Ineligible leads – established during screener	0	1	0	0
Ineligible leads – established pre-screener	0	1	0	0
Refusals	86	121	34	3
Unusable leads with working numbers	10	10	8	13
Unusable numbers	22	36	26	2
Working numbers with unknown eligibility	141	359	179	127
Expected eligibility of screened respondents	100%	99%	100%	100%
Expected eligibility of working numbers	100%	99%	100%	100%
Unadjusted response rate	34%	23%	16%	19%
Adjusted response rate	37%	25%	22%	19%
Cooperation rate	62%	57%	63%	90%

Response rates under COVID-19 and expected negligible impact on the survey reliability

The adjusted response rate for businesses (19%) and charities (32%) in the 2021 survey was lower than in the 2020 survey (27% and 45% respectively). The lower response rates are likely to be due to a combination of unique circumstances brought about by the COVID-19

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

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

restrictions, as well as the ongoing challenge of declining response rates in survey fieldwork in general. This survey's fieldwork overlapped with the third and fourth UK-wide lockdowns and with various other COVID-19 restrictions that affected the operations of most UK organisations. These restrictions and the overall environment under which fieldwork took place meant:

- It was harder to reach organisations via landline numbers as many switchboards were no longer running or had a skeleton service.
- When we did get through, it was harder to reach the right individual within the organisation, who may have been working remotely rather than in an office, or may have been placed on furlough.
- Where we did reach the right person, these individuals were often busier than in previous years due to the overall strain that the pandemic placed on IT and cyber teams. And they were consequently less willing to take part in surveys in general.

More generally, there has been an increasing awareness of cyber security, potentially making businesses more reticent to take part in surveys on this topic.

Furthermore, the increase in the survey length from c.17 minutes in 2020 to c.20 minutes this year is also expected to have reduced the response rate.

However, it is important to remember that response rates are not a direct measure of non-response bias in a survey, but only a measure of the potential for non-response bias to exist. Previous research into response rates, mainly with consumer surveys, has indicated that they are often poorly correlated with non-response bias.[15]

The idea of non-response bias entering the survey assumes that the organisations declining to take part are substantially different in terms of their cyber security approaches to the ones we did interview. If we believe, reasonably, that the response rates this year were mainly lower due to COVID-19 and associated restrictions, then we must consider whether the businesses most negatively impacted by COVID-19 are likely to have different cyber security challenges or require different approaches to the issue – we have no strong reasons to believe this.

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. In addition, respondents overwhelmingly revalidated their answers at the cost questions in the online follow-up survey. This meant that, typically, minimal work was needed to manually edit the data post fieldwork.

Nonetheless, individual outliers in the data can heavily affect cyber breach cost estimates. Therefore, the research team manually checked the final data for outliers and recalculated the estimates without these outliers, in order to check the impact that they were having on answers. This year, we opted to remove two responses from businesses from the COST question (total cost of all breaches or attacks identified in the last 12 months), where the respondents had stated the cost of breaches equalled £1,000,000. This was after judging whether these

[15] See, for example, Groves and Peytcheva (2008) "The Impact of Nonresponse Rates on Nonresponse Bias: A Meta-Analysis", Public Opinion Quarterly (available at: https://academic.oup.com/poq/article-abstract/72/2/167/1920564) and Sturgis, Williams, Brunton-Smith and Moore (2016) "Fieldwork Effort, Response Rate, and the Distribution of Survey Outcomes: A Multilevel Meta-analysis", Public Opinion Quarterly (available at: https://academic.oup.com/poq/issue/81/2).

responses were credible based on the size and nature of the business, and after checking with DCMS. The final SPSS data uploaded to the UK Data Archive excludes these 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

The education institutions samples are unweighted. Since they were sampled through a simple random sample approach, there were no sample skews to be corrected through weighting.

For the business and charities samples, we applied random iterative method (rim) weighting for two reasons. Firstly, to account for non-response bias where possible. Secondly, to account for the disproportionate sampling approaches, which purposely skewed the achieved business sample by size and sector, and the charities sample by income band. The weighting makes the data representative of the actual UK business and 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 here.

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 2020.

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 2.5 and Table 2.6 shows the unweighted and weighted profiles of the final data. The percentages are rounded so do not always add to 100 per cent.

Table 2.5: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Micro (1–9 staff)	52%	81%
Small (10–49 staff)	19%	15%
Medium (50–249 staff)	15%	3%
Large (250+ staff)	15%	1%
Sector		
Administration or real estate	14%	13%
Construction	8%	13%
Education	1%	1%
Entertainment, service or membership organisations	5%	7%
Finance or insurance	7%	2%
Food or hospitality	8%	10%
Health, social care or social work	8%	4%
Information or communications	7%	6%
Professional, scientific or technical	11%	14%
Retail or wholesale (including vehicle sales or repairs	16%	18%
Transport or storage	3%	4%
Utilities or production (including manufacturing)	11%	7%

Table 2.6: 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%	35%
£100,000 to under £500,000	17%	14%
£500,000 to under £5 million	22%	6%
£5 million or more	10%	2%
Unknown income	8%	6%
Country		
England and Wales	84%	85%
Northern Ireland	3%	3%
Scotland	13%	12%

2.7 SPSS data uploaded to UK Data Archive

A de-identified SPSS dataset from this survey is being published on the UK Data Archive to enable further analysis. The variables are consistent with those in the previously archived datasets (in 2020, 2019 and 2018), outside of new questions.

List of changes to old variables in the SPSS file

The following SPSS variables are no longer comparable with previous years due to significant changes in question wording (covered earlier in Section 2.1):

- RULES1
- MANAGE4
- COST_BANDS.

The following questions, which were present in the 2020 SPSS data, were removed from the survey questionnaire, but, we have kept the variable with blank data in the latest SPSS file to preserve the numeric ordering of variables in the file (e.g. since there is an POLICY8 variable, we have kept POLICY6 and POLICY7 rather than delete them). We have then relabelled these variables to make it clear they are no longer being used.

- MANAGE5
- IDENT8 to IDENT10
- POLICY6 to POLICY7
- PREVENT6, PREVENT8 to PREVENT11, PREVENT17 to PREVENT23 and PREVENT27 to PREVENT35.

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 of those who gave a response gave numeric responses (e.g. 81% at the COST question, after excluding refusals and those saying there was no cost incurred).

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 between £100 and £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 “£100 to 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. £300 for everyone saying “£100 to 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.

Redaction of cost data

No numeric £ variables will be included in the published SPSS 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 direct short-term cost of the most disruptive breach or attack (damagedirsx_bands)
- the estimated direct long-term cost (damagedirlx_bands)
- the estimated staffing cost (damagestaffx_bands)
- the estimated damage or disruption cost (damagelindx_bands)
- the estimated cost of all breaches identified in the last 12 months (cost_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.[16] Users may, therefore, see very minor differences in results between the SPSS dataset and the percentages in the main release and infographics, which consistently use the survey data tables. These should be differences of no more than one percentage point, and only occur on rare occasions.

2.8 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.

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

Chapter 3: Qualitative approach technical details

The qualitative strand of this research focused on businesses, charities and higher education institutions. The latter group was a new addition this year. It reflected the fact that the sample of achieved interviews with higher education institutions in the survey was very low, so DCMS agreed to use the qualitative strand to explore their cyber security approaches in greater depth.

3.1 Sampling

We took the sample for the 32 in-depth interviews from the quantitative survey. We asked respondents during the survey whether they would be willing to be recontacted specifically to take part in a further 45-minute interview on the same topic. In total, 1,002 businesses (68%) and 331 charities (71%) agreed to be recontacted. Of the 28 higher education institutions interviewed, 24 agreed to be recontacted.

Ultimately, we carried out interviews with:

- 17 businesses
- 8 charities
- 7 higher education institutions.

3.2 Recruitment quotas and screening

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

- a specific cyber security insurance policy
- undertaken a cyber security risk assessment
- formally reviewed supply chain cyber security risks (including for immediate suppliers and their wider supply chain)
- undertaken internal or external cyber security vulnerability audits
- adhered to external cyber security accreditations.

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 December 2020 and January 2021. We conducted the 32 interviews through a mix of telephone and Microsoft Teams calls. Interviews lasted around 45-60 minutes on average.

DCMS originally laid out their topics of interest for 2021. 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 thematic areas:

- changes in attitudes and priorities with regards to cyber security over time
- changes made as a result of the COVID-19 pandemic
- perceptions of the National Cyber Security Centre (NCSC) COVID-19-related guidance
- approaches to risk management, including how and why risk assessments and audits are carried out, and the impact these have on organisations
- the rationale behind choosing specific cyber security insurance policies, and the impact these have on organisations
- the rationale for having specific external cyber security accreditations, and the impact these have on organisations
- cyber security approaches with suppliers and how organisations might be managing wider supply chain risks.

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 C.

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)	1
F	Construction	1
G	Retail or wholesale (including vehicle sales and repairs)	3
H	Transport or storage	0
I	Food or hospitality	1
J	Information or communications	2
K	Finance or insurance	2
L, N	Administration or real estate	3
M	Professional, scientific or technical	1
P	Education (excluding state education institutions)	1
Q	Health, social care or social work	0
R, S	Entertainment, service or membership organisations	2
	Total	**17**

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)	8
Medium (49–249 staff)	4
Large (250+ staff)	5

Table 3.3 shows a profile of the 8 interviewed charities by income band.

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

Income band	Total
£100,000 to under £500,000	2
£500,000 to under £5 million	2
£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.

Chapter 4: Research burden

The Government Statistical Service (GSS) has a policy of monitoring and reducing statistical survey burden to participants where possible, and the burden imposed should be proportionate to the benefits arising from the use of the statistics. As a producer of statistics, DCMS is committed to monitoring and reducing the burden on those providing their information, and on those involved in collecting, recording and supplying data.

This section calculates the research compliance cost, in terms of the time cost on respondents, imposed by both the quantitative survey and qualitative fieldwork.

- The quantitative survey had **2,284 respondents** and the average (mean) survey length was **20 minutes**. Therefore the research compliance cost for the quantitative survey this year was [2,284 × 20 minutes = **761 hours**].
- The qualitative research had **30 respondents** and the average interview length was **55 minutes**. Respondents completed the qualitative interviews in addition to the quantitative survey. The research compliance cost for the qualitative strand this year was [30 × 55 minutes = **28 hours**].

In total, the compliance cost for the Cyber Security Breaches Survey 2021 was **789 hours**.

Steps taken to minimise the research burden

Across both strands of fieldwork, we took the following steps to minimise the research burden on respondents:

- making it clear that all participation was voluntary
- informing respondents of the average time it takes to complete an interview at the start of the survey call, during recruitment for the qualitative research and again at the start of the qualitative interview
- confirming that respondents were happy to continue if the interviews went over this average time
- offering to carry out interviews at the times convenient for respondents, including evenings and weekends where requested.

Appendix A: 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

ASK ALL
Q1B.TITLE
What is your job title?
PROMPT TO CODE, INCLUDING SENIORITY AND IF RELATED DIRECTLY TO CYBER SECURITY OR NOT

SINGLE CODE PER BOLD HEADING
Job title
Directly related to cyber security
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)
Director of Security
Head of Cyber Security/Information Security
Other cyber security role WRITE IN

Directly related to IT
Senior IT role (e.g. IT director)
Non-senior IT role (e.g. IT manager, technician, administrator)

Not related to cyber security/IT – senior management level
Business owner
Chief Executive (CEO)/Managing Director (MD)
Chief Operations Officer (COO)/Operations Director
Finance Director/Controller
Headteacher
Trustee/treasurer/on trustee board
Other senior management role (e.g. director)

Not related to cyber security/IT – non-senior management level
General/office manager (not a director/trustee)
PA/secretary/admin
Teacher (not in senior management)
Other non-senior role

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 [IF BUSINESS/EDUCATION: employees/IF CHARITY: 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)
IF BUSINESS/CHARITY: The ability for customers to order, book or pay for products or services online
IF CHARITY: The ability for people to donate online
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
IF SAMPLE SICVAR=1: An industrial control system
IF BUSINESS/CHARITY: Personal information about your [IF BUSINESS: customers/IF CHARITY: beneficiaries, service users or donors] held electronically
Network-connected devices like TVs, building controls, alarms, speakers etc., sometimes called smart devices
Computers with older versions of Windows installed (e.g. Windows 7 or 8)

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 currently use personally-owned devices, such as smartphones, tablets, or home computers to carry out regular work-related activities?

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

ASK ALL
Q9D.COVPRI
IF HALF A: Since the COVID-19 lockdown in March, has cyber security become a higher priority, a lower priority or has there been no change in its prioritisation for your organisation's [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management?
IF HALF B: Since the COVID-19 lockdown in March, has cyber security become a lower priority, a higher priority or has there been no change in its prioritisation for your organisation's [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management?
DO NOT READ OUT

SINGLE CODE
REVERSE SCALE
Higher priority
No change
Lower priority
Don't know

Q9E.COVIMPACTH DELETED POST-PILOT IN CSBS 2021

Q9F.COVIMPACTL DELETED POST-PILOT IN CSBS 2021

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

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

Q23Y.INSUREYES DELETED POST-PILOT IN CSBS 2021

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

Education related
Jisc/the Janet network
Department for Education (DfE)
Ofsted
Secure Schools programme
Teachers' unions (e.g. NASUWT, NEU or NUT)

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

Q24B.GOVTINF DELETED PRE-PILOT IN CSBS 2021

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 BUSINESS OR EDUCATION INSTITUTION ((SIZEDUM CODES 3–4 AND TYPEXDUM CODE 1) OR TYPEDUM CODE 3): The Cyber Security Board Toolkit
e. IF CHARITY (TYPEXDUM CODE 2): The Cyber Security Small Charity Guide
f. National Cyber Security Centre, or NCSC, guidance on secure home working or video conferencing
g. IF BUSINESS/CHARITY: National Cyber Security Centre, or NCSC, guidance for moving your business online

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

ASK IF SEEN OR HEARD GOVERNMENT GUIDANCE (CYBERAWARE CODE 1 OR ANY SCHEMEa-g CODE 1)
Q24E.GOVTACT
What, if anything, have you changed or implemented at your organisation after seeing or hearing any government campaigns or guidance on cyber security?
DO NOT READ OUT
PROBE FULLY ("ANYTHING ELSE?")

MULTICODE
Governance changes
Increased spending
Changed nature of the business/activities
New/updated business continuity plans
New/updated cyber policies
New checks for suppliers/contractors
New procurement processes, e.g. for devices/IT
New risk assessments
Increased senior management oversight/involvement

Technical changes
Changed/updated firewall/system configurations
Changed user admin/access rights
Increased monitoring
New/updated antivirus/anti-malware software
Other new software/tools (not antivirus/anti-malware)
Penetration testing

People/training changes
Outsourced cyber security/hired external provider
Recruited new staff
Staff training/communications
Vetting staff/extra vetting

Other WRITE IN

SINGLE CODE
Nothing done
Only heard about guidance, not read it

Don't know

Q25.TRAINA 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 your **current** cyber security processes and procedures. Just to reassure you, we are not looking for a "right" or "wrong" answer. If you don't do or have the things we're asking about, just say so and we'll move on.

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 that covers cyber security

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

ASK ALL
Q29A.COMPLY
Which of the following standards or accreditations, if any, does your organisation adhere to?
READ OUT

MULTICODE
ROTATE LIST BUT KEEP CODE 4 AND 5 TOGETHER
ISO 27001
The Payment Card Industry Data Security Standard, or PCI DSS
Any National Institute of Standards and Technology (NIST) standards
IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): The Cyber Essentials standard
IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): The Cyber Essentials Plus standard

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
A cyber security vulnerability audit
A risk assessment covering cyber security risks
Invested in threat intelligence
Used specific tools designed for security monitoring, such as Intrusion Detection Systems
Penetration testing
Testing staff awareness and response (e.g. via mock phishing exercises)

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

ASK IF CARRIED OUT AN AUDIT (IDENT CODE 1)
Q30A.AUDIT
Were any cyber security audits carried out internally by staff, by an external contractor, or both?
DO NOT READ OUT

SINGLE CODE
Only internally by staff
Only by an external contractor
Both internal and external
Don't know

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 11 MUST FOLLOW CODE 10
A policy to apply software security updates within 14 days
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
A virtual private network, or VPN, for staff connecting remotely
An agreed process for staff to follow when they identify a fraudulent email or malicious website

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)
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 cloud computing
Use of network-connected devices, sometimes called smart devices
Use of Software as a Service, or SaaS
How you're supposed to store data

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 3 months
3 to under 6 months ago
6 to under 12 months ago
12 to under 24 months ago
24 months ago or earlier
DO NOT READ OUT: Don't know

ASK ALL
Q33B.TRAINED
In the last 12 months, have you carried out any cyber security training or awareness raising sessions specifically for any [IF BUSINESS/EDUCATION: staff/IF CHARITY: staff or volunteers] who are not directly involved in cyber security?

SINGLE CODE
Yes
No
Don't know

Q33C.COVREVIEW DELETED POST-PILOT IN CSBS 2021

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 BUSINESSES
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.

READ OUT TO CHARITIES OR EDUCATION
The next question is about third-party organisations you work with. This includes any immediate suppliers that directly provide goods or services to your organisation, or partners such as local authorities. 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 [IF CHARITY/EDUCATION: or partners]
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

ASK IF REVIEWED ANY SUPPLY CHAIN RISKS (CODE 1 AT SUPPLYRISKA OR SUPPLYRISKB)
Q45D.BARRIER
Which of the following, if any, have made it difficult for your organisation to manage any cyber security risks from your supply chain [IF CHARITY/EDUCATION: or partners]?
READ OUT

MULTICODE
RANDOMISE LIST
Lack of time or money to dedicate to this
Lack of skills to be able to check suppliers [IF CHARITY/EDUCATION: or partners] in this way
Not knowing what kinds of checks to carry out
Not knowing which suppliers [IF CHARITY/EDUCATION: or partners] to check
We can't get the necessary information from suppliers [IF CHARITY/EDUCATION: or partners] to carry out checks
It's not a priority when working with suppliers [IF CHARITY/EDUCATION: or partners]

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

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

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
CODES 7, 8 AND 9 TO STAY IN ORDER
Computers becoming infected with ransomware
Computers becoming infected with other malware (e.g. viruses or spyware)
Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services
Hacking or attempted hacking of online bank accounts
People impersonating your organisation in emails or online
Phishing attacks, i.e. staff receiving fraudulent emails, or arriving at fraudulent websites
Unauthorised accessing of files or networks by **staff**, even if accidental
IF EDUCATION: Unauthorised accessing of files or networks by **students**
Unauthorised accessing of files or networks by **people** [IF BUSINESS/CHARITY: **outside your organisation**/IF EDUCATION: **other than staff or students**]
Unauthorised listening into video conferences or instant messaging
Takeovers or attempts to take over your website, social media accounts or email accounts

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 1–12)
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 1–12)
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
CODE 7 MUST FOLLOW CODE 6
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
Money was paid as a ransom
Your website, applications or online services were taken down or made slower
Lost access to any third-party services you rely on
Physical devices or equipment were damaged or corrupted
Compromised accounts or systems used for illicit purposes (e.g. launching attacks)

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 1–12)
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
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]
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

Q57A.OUTIMPTYPE DELETED POST-PILOT IN CSBS 2021

Q58.MONITOR DELETED PRE-PILOT IN CSBS 2018

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 the incident
An assessment of the scale and impact of the incident
Communications and public engagement plans
Debriefs to log any lessons learnt

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 1–12)
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.DISRUPT DELETED PRE-PILOT IN CSBS 2017

ASK IF MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE TYPE CODES 1–12)
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

SINGLE CODE
CODES MENTIONED AT TYPE
Computers becoming infected with ransomware
Computers becoming infected with other malware (e.g. viruses or spyware)
Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services
Hacking or attempted hacking of online bank accounts
People impersonating your organisation in emails or online
Phishing attacks, i.e. staff receiving fraudulent emails or arriving at fraudulent websites
Unauthorised accessing of files or networks by **staff**, even if accidental
Unauthorised accessing of files or networks by **students**

Unauthorised accessing of files or networks by **people** [IF BUSINESS/CHARITY: **outside your organisation**/IF EDUCATION: **other than staff or students**]
Unauthorised listening into video conferences or instant messaging
Takeovers or attempts to take over your website, social media accounts or email accounts
Any other types of cyber security breaches or attacks
DO NOT READ OUT: Don't know

READ OUT IF EXPERIENCED ONE TYPE OF BREACH OR ATTACK MORE THAN ONCE ([ONLY 1 TYPE CODES 1–12] 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.

Q65.IDENTB DELETED PRE-PILOT IN CSBS 2021

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 1–12] 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

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 DELETED PRE-PILOT IN CSBS 2021

Q75B.DAMAGEDIRB DELETED PRE-PILOT IN CSBS 2021

Q75C.DAMAGEREC DELETED PRE-PILOT IN CSBS 2021

Q75D.DAMAGERECB DELETED PRE-PILOT IN CSBS 2021

Q75E.DAMAGELON DELETED PRE-PILOT IN CSBS 2021

Q75F.DAMAGELONB DELETED PRE-PILOT IN CSBS 2021

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–12] 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 1–12] 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 1–12] 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
Governance changes
Increased spending
Changed nature of the business/activities
New/updated business continuity plans
New/updated cyber policies
New checks for suppliers/contractors
New procurement processes, e.g. for devices/IT
New risk assessments
Increased senior management oversight/involvement

Technical changes
Changed/updated firewall/system configurations
Changed user admin/access rights
Increased monitoring
New/updated antivirus/anti-malware software
Other new software/tools (not antivirus/anti-malware)
Penetration testing

People/training changes
Outsourced cyber security/hired external provider
Recruited new staff
Staff training/communications
Vetting staff/extra vetting

Other WRITE IN

SINGLE CODE
Nothing done
Don't know

READ OUT IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–12] OR DISRUPTA NOT DK)
I am now going to ask you about the approximate costs of this particular breach or attack.

ASK IF ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ([ONLY 1 TYPE CODES 1–12] OR DISRUPTA NOT DK)
Q78K.DAMAGEDIRS
What was the approximate value of any external payments made **when the incident was being dealt with**? This includes:

- any payments to external IT consultants or contractors to investigate or fix the problem
- any payments to the attackers, or money they stole.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£999,999
SOFT CHECK IF >£9,999

SINGLE CODE
No cost of this kind incurred
Don't know
Refused

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEDIRSHO CODE DK)
Q78L.DAMAGEDIRSB
Was it approximately … ?
PROMPT TO CODE

SINGLE CODE
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 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 1–12] OR DISRUPTA NOT DK)
Q78M.DAMAGEDIRL
What was the approximate value of any external payments made **in the aftermath** of the incident? This includes:

- any payments to external IT consultants or contractors to run audits, risk assessments or training
- the cost of new or upgraded software or systems
- recruitment costs if you had to hire someone new
- any legal fees, insurance excess, fines, compensation or PR costs related to the incident.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£999,999
SOFT CHECK IF >£9,999

SINGLE CODE
No cost of this kind incurred
Don't know
Refused

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEDIRLONG CODE DK)
Q78N.DAMAGEDIRLB
Was it approximately … ?
PROMPT TO CODE

SINGLE CODE
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 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 1–12] OR DISRUPTA NOT DK)
Q78O.DAMAGESTAFF
What was the approximate cost of the **staff time** dealing with the incident? This is how much staff would have got paid for the time they spent investigating or fixing the problem. Please include this cost even if this was part of this staff member's job.
PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£999,999
SOFT CHECK IF >£9,999

SINGLE CODE
No cost of this kind incurred
Don't know
Refused

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMINDIRSHO CODE DK)
Q78P.DAMAGESTAFFB
Was it approximately … ?
PROMPT TO CODE

SINGLE CODE
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 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 1–12] OR DISRUPTA NOT DK)
Q78Q.DAMAGEIND
What was the approximate value of any **damage or disruption** during the incident? This includes:

- the cost of any time when staff could not do their jobs
- the value of lost files or intellectual property
- the cost of any devices or equipment that needed replacing.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£999,999
SOFT CHECK IF >£9,999

SINGLE CODE
No cost of this kind incurred
Don't know
Refused

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMINDIRLONG CODE DK)
Q78R.DAMAGEINDB
Was it approximately … ?
PROMPT TO CODE

SINGLE CODE
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 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 ANY BREACHES OR ATTACKS (TYPE CODES 1–12)
Q59.COSTA
Considering all these different costs, how much do you think **all** the cyber security breaches or attacks you have experienced in the last 12 months have cost your organisation financially?
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 >£9,999
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 >£99,999

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 … ?
PROMPT TO CODE

SINGLE CODE
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 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

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 IF ANY BREACHES OR ATTACKS AND NOT REFUSED ALL COST QUESTIONS (TYPE CODES 1–12 AND NOT [DAMAGEDIRS, DAMAGEDIRL, DAMAGESTAFF, DAMAGEIND AND COSTA ALL REF])
Q78K.VALIDATE
We'd like to send you a quick email afterwards giving you the chance to validate the answers at those last questions, as we know you may want to check them again. It really helps us to get accurate cost data from this survey, so we can properly report the impact of these kinds of cyber attacks.

This email will also have a link to last year's report and a Government help card, showing the latest official cyber security guidance for organisations like yours, including under COVID-19.

Are you happy for us to email you?

SINGLE CODE
Yes
No

ASK ALL
Q79.RECON
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 2021?

SINGLE CODE
Yes
No

ASK IF NO BREACHES OR ATTACKS OR REFUSED ALL COST QUESTIONS (TYPE CODES DK, NULL OR REF AND [DAMAGEDIRS, DAMAGEDIRL, DAMAGESTAFF, DAMAGEIND AND COSTA ALL REF])
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 IF WANT RECONTACT OR REPORT/HELPCARD (RECON CODE 1 OR REPORT 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
SEND WEB INVITE IF VALIDATE 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

Web follow-up

SHOW IF ELIGIBLE FOR WEB SURVEY (VALIDATE CODE 1)
Thanks for taking part. The next screens give you the chance to recheck or correct any cost information you gave us in the telephone survey.

You may want to talk to IT or finance colleagues to ensure you give accurate answers.

ASK IF ANSWERED ONE OF THE DISRUPTIVE BREACH COST QUESTIONS ((DAMAGEDIRSB NOT DK AND DAMAGEDIRS NOT REF OR NULL) OR (DAMAGEDIRLB NOT DK AND DAMAGEDIRL NOT REF OR NULL) OR (DAMAGESTAFFB NOT DK AND DAMAGESTAFF NOT REF OR NULL) OR (DAMAGEINDB NOT DK AND DAMAGEIND NOT REF OR NULL))
Q82.CHECKA
You said the most disruptive cyber security breach or attack you had in the last 12 months was: [ANSWER AT DISRUPTA].

It is important that we get accurate cost data for this breach or attack, so the Government can properly understand the impact of cyber attacks on organisations like yours. Please let us know if the responses below are correct or incorrect.

ASK AS A COLLAPSABLE GRID

a. IF DAMAGEDIRSB NOT DK: You said the approximate value of any external payments made **when the incident was being dealt with** was **[ANSWER AT DAMAGEDIRS OR DAMAGEDIRSB]**. This includes:
    - any payments to external IT consultants or contractors to investigate or fix the problem
    - any payments to the attackers, or money they stole.
b. IF DAMAGEDIRLB NOT DK: You said the approximate value of any external payments made **in the aftermath** of the incident was **[ANSWER AT DAMAGEDIRL OR DAMAGEDIRLB]**. This includes:
    - any payments to external IT consultants or contractors to run audits, risk assessments or training
    - the cost of new or upgraded software or systems
    - recruitment costs if you had to hire someone new
    - any legal fees, insurance excess, fines, compensation or PR costs related to the incident.
c. IF DAMAGESTAFFB NOT DK: You said the approximate cost of the **staff time** dealing with the incident was **[ANSWER AT DAMAGESTAFF OR DAMAGESTAFFB]**. This is how much staff would have got paid for the time they spent investigating or fixing the problem. Please include this cost even if this was part of this staff member's job.
d. IF DAMAGEINDB NOT DK: You said the approximate value of any **damage or disruption** during the incident was **[ANSWER AT DAMAGEIND OR DAMAGEINDB]**. This includes:
    - the cost of any time when staff could not do their jobs
    - the value of lost files or intellectual property
    - the cost of any devices or equipment that needed replacing.

SINGLE CODE
Correct
Incorrect

ASK IF ANSWERED TOTAL COST QUESTION (COSTB NOT DK AND COSTA NOT REF OR NULL)
Q82.CHECKB
You said that **all** the cyber security breaches or attacks you have experienced in the last 12 months have cost your organisation **[ANSWER AT COSTA OR COSTB]**.

Please let us know if this response is correct or incorrect.

SINGLE CODE
Correct
Incorrect

ASK IF DAMAGEDIRSB CODE DK OR CHECKAa CODE 2
CLONE OF DAMAGEDIRS

CLONE OF DAMAGEDIRSB

ASK IF DAMAGEDIRLB CODE DK OR CHECKAb CODE 2
CLONE OF DAMAGEDIRL
CLONE OF DAMAGEDIRLB

ASK IF DAMAGESTAFFB CODE DK OR CHECKAc CODE 2
CLONE OF DAMAGESTAFF
CLONE OF DAMAGESTAFFB

ASK IF DAMAGEINDB CODE DK OR CHECKAd CODE 2
CLONE OF DAMAGEIND
CLONE OF DAMAGEINDB

ASK IF COSTB CODE DK OR CHECKB CODE 2
CLONE OF COSTA
CLONE OF COSTB

SHOW IF ELIGIBLE FOR WEB SURVEY (VALIDATE CODE 1)
Thank you for taking the time to participate in this study. 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 B: Help card offered to survey respondents

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.

Cyber Security in Schools – https://www.ncsc.gov.uk/information/resources-for-schools

These cards have been designed to help all those who work in schools understand what cyber security is, how it's relevant and what steps they can take to raise their school's resilience to cyber incidents.

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.

Appendix C: 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 by the Department for Digital, Culture, Media & Sport (DCMS) ● Explain the research: we are speaking with organisations to learn more about how they approach cyber security and to discuss topics from the survey in more detail ● 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 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 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**
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.*

Cyber security since March 2020 and COVID-19 impact so far	**10-12 minutes**
Has your organisation made any changes or adaptations to the way you work and your digital infrastructure since the first UK lockdown in March 2020? PROBE: ● Home working/VPNs ● Moving business/services online ● New IT systems/servers ● New software/hardware How have you considered the cyber security risks of these changes? ● How have you assessed the risks? Formal risk assessments? Have you had any help/extra resources to do this? ● How aware are senior managers/the board of these risks? ● How aware are wider staff? IF NOT CONSIDERED THE CYBER RISKS: Why haven't these been considered? PROBE: ● Lack of resources/time ● Support/guidance needed And how has cyber security in your organisation changed since the first UK lockdown? PROBE: WHAT THEY HAVE DONE: ● New policies/processes ● Changes to existing policies/processes ● Changes to budgets/investment in cyber security WHO HAS BEEN INVOLVED: ● Staffing/cyber security teams ● Outsourcing/use of contractors/consultants for cyber security ● Senior managers/board engagement with new measures CHANGES IN ATTITUDES: ● Attitudes of senior managers towards cyber security ● Attitudes of wider staff towards cyber security ● Changes to cyber security training/awareness raising In the survey you said that COVID-19 had led to cyber security become a higher/lower priority within your organisation? Why was this? How cyber secure would you say you are given all the changes that have taken place since March 2020? ● Have any aspects of cyber security improved? ● Has anything got worse or harder to maintain? ● What are the ongoing/new risks? What have been the main cyber security challenges since March 2020? How have you approached these? What has worked well? Less well?	*This section focuses on how cyber security has changed since the start of the COVID-19 pandemic and lockdown, the challenges this has raised and how the organisation has responded.*

Cyber security changes within organisations before COVID-19 and drivers of these changes	**7-8 minutes**
Now I'd like to focus on how cyber security was developing in your organisation before the COVID-19 pandemic. Since the start of 2019 and up to March 2020, how did cyber security evolve in your organisation? PROBE ANY CHANGES IN: ● Higher/lower prioritisation ● Budgets/investment ● Policies/processes ● Staffing/cyber security teams ● Senior manager/board attitudes/engagement ● Staff attitudes/culture towards cyber security What have been the main drivers behind these changes before March 2020? What triggered any improvements? What led to a reduced focus on cyber security over this time? PROBE IMPACT/INFLUENCE OF EACH OF THE FOLLOWING: MOST IMPORTANT TO PROBE: ● Cyber incidents/breaches and reaction to these ● Shareholders/investors demanding/asking about it ● Changes in your competitors/peers – benchmarking to others in the industry ● Business environment (e.g. economic downturn, EU exit) PROBE IF TIME: ● Media stories about cyber security ● Changes in tech/digitisation/moves online ● Changing organisation priorities ● Compliance/regulator demands ● Trying to achieve a specific standard (PROBE WHY) ● Customers demanding/asking about it IF NOT PROBED ABOVE: Since the start of 2019, how have any investors or shareholders influenced cyber security in your organisation? Have they led to any changes in your approach? IF NOT RAISED ABOVE: Are there any aspects of cyber security that you have reduced focus on since the start of 2019? What has driven this?	*This section looks at the direction of travel of cyber security before March 2020 (i.e. how things were already changing before the pandemic). We want to understand the drivers behind these changes.*
Planned future changes to cyber security over the next 12 months	**7-8 minutes**
Now I'd like to focus on how you expect cyber security to develop in your organisation over the next 12 months. What changes do you expect to happen in this time? Why is this? Are these changes you are already planning for? ● How are you planning for them? ● Who is involved in decision making? ● What challenges do you anticipate? ● What guidance have you sought? ● What kind of help/support/guidance might you need/find useful? How permanent are these changes?	*This section looks at the further changes organisations expect to make to cyber security in the next 12 months, which changes are likely to be permanent or temporary and the challenges they foresee.*

Government guidance	**6-7 minutes**
We sent you some links to government guidance on cyber security before this interview and asked you to take a look. Which ones have you looked at? REFER TO SAMPLE AND USE ALLOCATED PIECE OF GUIDANCE. What did you think of these? ● Who is this aimed at? PROBE: People in cyber roles, senior managers/directors, anyone else in the business ● How relevant is this guidance for your organisation? How much does it address your cyber security needs? What questions/support needs do you still have? ● What do you like about it? What works well? ● What works less well? What could be improved? What would your organisation do after seeing this guidance? ● Would it prompt you to do differently/make any changes? Would it prompt any internal discussions/checks?	*What do organisations think of NCSC guidance on COVID-19?* *Is it relevant to them? Could it be improved? What difference would it make to their approach?*

N.B. you will only have to ask up to two of these 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. risk assessment is the top priority).

SECTION ONLY RELEVANT IF FLAGGED RED IN THE SAMPLE (PRIORITY #1): Risk assessment	**10 minutes**
In the survey, you mentioned that you have undertaken a cyber security risk assessment. Can you describe what this involves? ● What information does your organisation use to inform a cyber security risk assessment? ● What aspects do you focus on? PROBE: technical controls, staff attitudes/behaviour, external data/intelligence ● Who carries them out? Do you involve anyone outside the organisation? Could your risk assessments process be improved? ● How thorough is the process? ● What support would be helpful? What do you hope to achieve from risk assessments? How do you ensure you act on the findings? In your last cyber security risk assessment, what did you find? What did you implement/change as a result? Are there any things that stopped you from acting on the identified risks? Do cyber security risk assessments have any other impacts or benefits? PROBE IMPACT ON: ● Changing staff behaviour ● Senior manager/board attitudes ● Signalling to regulators/customers/investors ● Improved reputation	*What kind of risk assessments are organisations taking?* *What's the RoI in monitoring and identifying cyber risks?*

SECTION ONLY RELEVANT IF FLAGGED GREY IN THE SAMPLE (PRIORITY #2): Supply chain risk management	**10 minutes**
In the survey, you said you had formally reviewed the cyber risks presented by your supply chain. How have you done this? How well would you say you understand your suppliers' cyber security practices? ● Are there any gaps in your knowledge/understanding? ● How much do you understand this for the wider supply chain? What challenges have you faced when dealing with cyber security risks from suppliers? PROBE: ● Ability to monitor (e.g. technical knowledge/skills) ● Time/resources ● Impact on supplier relationships ● Knowing what good looks like/acceptable standards How have you addressed these challenges? ● How easy/difficult has it been to address these challenges? ● Are there different challenges for immediate suppliers vs. your wider supply chain? How easy is it to manage wider supply chain risks? What kinds of support/guidance might help you to overcome these challenges/better manage these cyber risks? ● What kinds of government support/guidance would help? Do you treat different types of suppliers the same/differently when it comes to cyber security? ● How do you differentiate? Why is it important for these suppliers? ● What kinds of suppliers/parts of the supply chain pose most risk to cyber security? What happens if they don't fulfil their responsibilities? What would happen if a supplier had a cyber security incident? ● How would you know? ● Who is responsible? ● What action would you take during/after the incident? ● How likely is this to happen? How much control do you have over it?	*How do organisations manage supplier/wider supply chain cyber risks?* *What challenges do organisations face when managing risk from suppliers and the wider supply chain? What might help them with these challenges?* *How do organisations categorise suppliers in terms of cyber risk?*

SECTION ONLY RELEVANT IF FLAGGED BROWN IN THE SAMPLE (PRIORITY #3): Cyber Insurance	**10 minutes**
In the survey, you mentioned that you have a specific cyber insurance policy. What was the motivation behind taking out this policy? ● Why was it important to have a standalone policy vs. just adding coverage within a wider business insurance policy? What does your cyber insurance cover? What are the key/essential things you wanted it to cover? What impact has having cyber insurance had on your organisation's approach to cyber security? PROBE: ● Would you have done anything differently if you didn't have this insurance policy? ● Has it led to increased monitoring/risk assessment? ● Have you adopted new controls? ● Have you adopted any standards? ● New training/awareness raising? Does your insurance policy mandate you to do any of these things, or have you chosen to do them? Did you have to raise your cyber security standards/change your approaches to be eligible for the policy or did your existing approach already qualify? How would you expect your insurance provider to help you if you made a claim? What would you have to provide? Under what circumstances would you make a claim? PROBE: ● If above a certain financial threshold? ● Certain types of breaches/attacks? ● When would it not be worth your while claiming?	*Why are organisations getting cyber specific insurance? What does a standalone policy look like?* *Are there any positive behavioural impacts from having cyber insurance? Does it mandate or encourage better cyber security?* *How would they expect a claims process to pan out and would it be worth it?*

SECTION ONLY RELEVANT IF FLAGGED BLUE IN THE SAMPLE (PRIORITY #4): Audits	**10 minutes**
You mentioned in the survey that your organisation has undertaken a cyber security vulnerability audit. What did this involve? • Did you develop this audit process yourself or bring in external expertise? • How long has it been in place? Has it evolved over time? What were the reasons behind any changes? 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? Who carries out the audit? IF INTERNAL: • Internal/external people involved? • What team are they in (HR, IT, other)? • What skills/qualifications do they have? IF EXTERNAL: • Why did you decide to get it done externally? • How did you find/choose your auditor? What's the main purpose of the audit? PROBE: • Being more resilient • Changing staff behaviour • Signalling to regulators/customers/investors • Improved reputation What do you do after the audit? Who is it reported to? What do they do with this information? PROBE: • Internal reporting • External reporting (e.g. annual reports) • Board involvement/interest • Insurance companies • Compliance/regulators • External bodies What happened after your last audit? What did you find? What changes did it lead to?	*How do organisations do cyber security audits? How have they developed the process?* *What's the rationale for doing it internally or externally?* *What do these audits achieve? Who are they for? What changes do they bring about?*

SECTION ONLY RELEVANT IF FLAGGED GREEN IN THE SAMPLE (PRIORITY #5): Accreditations	**10 minutes**
You mentioned in the survey that you had cyber security related accreditations or standards (LOOK AT RECRUITMENT PROFILE). What was the motivation behind getting the accreditation(s) you have? PROBE: ● Being more resilient ● Changing staff behaviour ● Signalling to regulators/customers/investors ● Improved reputation ● Competitors/peers have them, or it's typical for our sector What impact has this accreditation had on your organisation? ● Has it led to any changes in your cyber security? ● Have you been able to mitigate cyber risks better? ● Would you be doing anything differently if you didn't have this accreditation/standard? Are you aware of other cyber security accreditations/standards? Why did you choose this over those? What are the comparative advantages? PROBE: ● ISO 27001 ● PCI DSS ● NIST standards ● Cyber Essentials/Cyber Essentials Plus Do you comply with multiple cyber security accreditations/ standards? If so, why?	*What kind of accreditations do organisations see as important? Why is this?* *What impact does having accreditations have on an organisation's cyber security?*

NOW ASK ALL INTERVIEWEES THE BELOW SECTIONS

Wrap up	**2-3 minutes**
Overall, what do you think is the one thing I should take away from the discussion today? THANK AND CLOSE	*Wrap up the interview.*

Appendix D: 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
   - Orla Leggett, Ipsos MORI
   - Nick Coleman, Ipsos MORI
   - Jayesh Navin Shah, Ipsos MORI
   - Professor Steven Furnell, University of Nottingham.

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

3. The responsible DCMS analyst for this release is Emma Johns. The responsible statistician is Harry Smart. For enquiries on this release, from an official statistics perspective, please contact Harry at evidence@dcms.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