Department for Digital, Culture, Media & Sport

Ipsos

Cyber Security Breaches Survey 2022

Technical Annex

This Technical Annex provides the technical details of the Cyber Security Breaches Survey 2022. It covers the quantitative survey (fieldwork carried out in winter 2021 and 2022) and qualitative element (carried out in early 2022), 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 an influential research study for UK cyber resilience, aligning with the National Cyber Strategy. It is primarily used to inform government policy on cyber security, making the UK cyberspace a secure place to do business. The study explores the policies, processes and approach to cyber security, for businesses, charities and educational institutions. It also considers the different cyber attacks these organisations face, as well as how these organisations are impacted and respond.

For this latest release, the quantitative survey was carried out in winter 2021/22 and the qualitative element in early 2022.

Responsible analyst:

Maddy Ell
07825025654

Responsible statistician

Robbie Gallucci

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 2022:

- We undertook a random probability telephone survey of 1,243 UK businesses, 424 UK registered charities and 490 education institutions from 20 September 2021 to 21 January 2022. The data for businesses and charities have been weighted to be statistically representative of these two populations.
- We carried out 35 in-depth interviews across December 2021 and January 2022, 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 study.

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 2022 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-only surveys)
- a comprehensive attempt to obtain accurate 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).

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 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.
- The business survey intends to represent businesses of all sizes. As the BEIS Business Population Estimates 2021 show, the UK business population is predominantly made up of micro and small businesses. This presents a challenge – these businesses, due to their smaller scale and resource limitations, typically have a less mature cyber security profile. This may limit the insights this study in isolation can generate into the more sophisticated cyber security issues and challenges facing the UK's large business population, and the kinds of high-impact cyber security incidents that appear in the news and media. Nevertheless, the study design attempts to balance this by boosting survey responses among medium and large businesses (and high-income charities) and by focusing on larger organisations in the qualitative strand. Moreover, DCMS undertakes a separate survey series focused on larger organisations, the Cyber Security Longitudinal Survey, partly to address this limitation.
- Organisations may be inclined to give answers that reflect favourably on them in surveys about cyber security (a form of social desirability bias), given the common perceptions of reputational damage associated with cyber security incidents. Furthermore, organisations that have suffered from more substantial cyber security incidents may be less inclined to take part because of this. This may result in surveys like this one undercounting the true extent and cost of cyber security incidents. However, we make a concerted effort to overcome this in the administration of the survey. We make it clear to respondents, across a range of communication materials, that their answers are confidential and anonymous.
- A significant challenge remains in terms of designing a methodology that accurately captures the financial implications of cyber security incidents, given that survey findings necessarily depend on self-reported costs from organisations. As previous years' findings and wider DCMS research on the full cost of cyber security breaches suggest, there is no consistent framework across organisations at present that supports them to understand and monitor their costs, and many organisations do not actively monitor these costs at all. Moreover, we consciously opted to not to ask about certain long-term indirect costs (see Section 2.1), as it was unrealistic to collect accurate figures for these areas in a single survey. In addition, a survey based on a sample such as this one may miss some of the most financially damaging cyber security incidents, that affect a very small number of UK organisations in a very extreme way. This implies that respondents may underestimate the total cost of all breaches or attacks in the survey, and that our averaged results may miss critical cases within the population.

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 methodology is intended to be as comparable as possible to previous surveys in the series.

Across the years, there have, nonetheless, been some significant changes for readers to be aware of:

- In 2022, for the first time, we included the agriculture, forestry and fishing sector. In previous years, we have excluded this sector on the basis that these businesses were less likely to have any IT capacity or online presence. This is a small sector, accounting for 3.6 per cent of all UK businesses. As such, we expect the inclusion of this sector to have a negligible impact on the comparability of findings across years.
- The charities sample was added in 2018, while the education institutions sample was added in 2020. The initial education institutions sample in 2020 The scope of the school and college samples were expanded to include institutions in Wales, Scotland and Northern Ireland, as well as England.
- We achieved fewer business interviews this year (down from 1,419 last year to 1,243 in the 2022 survey). This includes fewer medium (149, vs. 210 in 2021) and large businesses (135, vs. 203 in 2021). This is primarily a reflection of the increasingly challenging business survey environment in the aftermath of the COVID-19 pandemic.
- We also achieved fewer further education interviews this year (34, vs. 57 in 2021). This also reflected the challenging situation of surveying schools and colleges generally at the start of a new term, during the release of new COVID-19 guidance for education settings.[1]
- By contrast, we increased the sample sizes for charities (from 337 to 424), primary schools (from 135 to 198), secondary schools (from 158 to 221) and higher education institutions (from 28 to 37). The higher sample sizes allow for more granular analysis by income band for charities. They also allow for more statistically reliable results for primary schools, secondary schools and higher education colleges – the latter group could not be reported in a statistically reliable way last year, since the achieved sample size was under 30. There is more discussion around the implications of the changes of sample sizes and associated margins of error in Section 2.5.
- The government's 10 Steps to Cyber Security guidance was refreshed between the 2021 and 2022 studies. The overall guidance covers much of the same ground, but the individual 10 Steps have been updated. In some cases, the themes are unchanged – for example, incident management remains one of the 10 Steps. In some cases, a theme has been refreshed or broadened, for instance with aspects of the previous "managing user privileges" step being absorbed into a new step around "identity and access management". Finally, some of the new steps cover entirely new themes, such as supply chain security. Consequently, DCMS and Ipsos decided this year to change the way the survey questions are mapped to the 10 Steps. This is detailed in Section 2.7.
- In 2021, 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 we cannot make direct comparisons between data from 2021 onwards 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.

[1] See, for example, the list of government COVID-19 guidance for further education colleges in England: https://www.gov.uk/government/collections/further-and-higher-education-coronavirus-covid-19.

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

1.5 Extrapolating results to the wider population

The survey results are weighted to be representative of the UK populations of businesses and charities. Therefore it is theoretically possible to extrapolate survey responses to the wider population (with the exception of the financial cost data, explained at the end of this section).

- The size of the total business population at the time of this study (excluding businesses with 0 employees, which were out of scope for this study) comes the BEIS Business Population Estimates 2021. This indicates a population of 1,414,980 UK businesses.
- The size of the registered charity population at the time of this study comes from combining the lists of registered charities across the 3 UK charity regulator databases (laid out in Section 2.3). This indicates a population of 200,203 registered charities.

We recommend accounting for the margin of error in any extrapolated results. The overall business sample this year has a margin of error range of ±2.1 to ±3.4 percentage points, based on a 95% confidence interval calculation. That is to say, if we were to conduct this survey 100 times (each time with a different sample of the business population), we would expect the results to be within 2.1 to 3.4 percentage points of the results we achieved here in 95 out of those 100 cases. The range illustrates that survey results closer to 50% tend to have higher margins of error. For example, if 90% of surveyed businesses said cyber security is a high priority for their senior management, this result would have a margin of error of ±2.1 percentage points, whereas if only 50% this, the margin of error would be ±3.4 percentage points.

The overall charities sample this year has a margin of error range of ±3.6 to ±6.0 percentage points (tending towards the higher end of that range for survey results closer to 50%).

We also recommend restricting any extrapolation to these overall populations rather than to any subgroups within these populations (e.g. large businesses, or construction businesses). The sample sizes for these subgroups in our survey are much smaller than the overall sample sizes, and consequently have much higher margins of error.

Any extrapolated results should be clearly labelled as estimates and, ideally, should be calibrated against other sources of evidence.

We specifically do not consider the financial cost estimates from this survey to be suitable for this sort of extrapolation (e.g. to produce a total cost for the UK economy). These estimates tend to have a high level of statistical standard error, so the margins of error for any extrapolated cost estimate are likely to be very wide, limiting the value of such an estimate.

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

If you wish to use extrapolated Cyber Security Breaches Survey data as part of your analysis or reporting, then we would encourage you to contact DCMS via the evidence mailbox: evidence@dcms.gov.uk.

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

The questionnaire content is largely driven by the Cyber Resilience team at DCMS. They ensure that the focus aligns with the National Cyber Strategy, to provide evidence on UK cyber resilience, and influence future government policy and other interventions in this space.

Ipsos 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 2021:

- stakeholder engagement via email with industry and government representatives
- cognitive testing interviews with 10 organisations (businesses, charities and schools)
- a pilot survey, consisting of 28 interviews (10 businesses, 12 charities and 6 schools).

A full list of all questionnaire amends since the 2021 study is included at the end of this section.

Stakeholder engagement

Each year, Ipsos has consulted a range of industry stakeholders, to ensure that the Cyber Security Breaches Survey continues to explore the most important trends and themes that organisations are grappling with when it comes to cyber security. This includes 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). Similarly, DCMS has consulted a range of stakeholders across government, such as the Home Office, the Treasury and the National Cyber Security Centre (NCSC).

In previous iterations, the questionnaire has undergone a more thorough revamp (e.g. in the 2021 study, the questions measuring the cost of breaches substantially changed). In these years, we have hosted questionnaire development workshops and stakeholder interviews, to gain in-depth insights from stakeholders, and to allow them to discuss ideas as a group.

This time, the changes to the questionnaire were expected to be minimal. Reflecting this, the stakeholder engagement approach was more light touch. Ipsos emailed the industry stakeholders that had been involved in previous years to solicit their written feedback on the quantitative and qualitative topics to be included in the study. Similarly, DCMS engaged over email with government stakeholders and passed this feedback to Ipsos. Separately, Ipsos and DCMS jointly held meetings with two stakeholders that had relationships with cyber security professionals in the further and higher education sectors – Jisc (a membership organisation of individuals in digital roles within the further and higher education sectors) and UCISA (formerly known as the Universities and Colleges Information Systems Association) – in order to refine our approach to engaging with these sectors from previous years. The engagement with Jisc and UCISA is detailed further in Section 2.4 (around maximising the response rate).

Questionnaire changes following stakeholder engagement

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

- the use of Managed Service Providers (at ONLINE)
- having a list of critical data, systems or assets (at MANAGE)
- the use of two-factor authentication (2FA, at RULES)
- whether organisations have a cyber security strategy (STRATEGY)

- whether this has been reviewed by senior management in the last 12 months (STRATINT) as well as by third parties outside the organisation (STRATEXT), and whether this review was specific to cyber security or a more general policy review (STRATREV)
- the reporting of cyber security risks in annual reports (CORPRISK), where organisations had published annual reports in the last 12 months (CORPORATE)
- whether organisations have a rule or policy to pay out in the case of ransomware attacks (RANSOM).

The questions around incident management approaches were split and expanded to cover a wider range of actions, resulting in new measures for the following actions or behaviours this year (at the existing INCIDCONTENT question and a new INCIDACTION question):

- formal incident response plans
- guidance around external reporting
- keeping internal records of incidents
- informing senior management of incidents
- informing regulators of incidents
- informing cyber insurance providers of incidents.

The entire incident management section of the questionnaire was also moved to be after the cost of breaches questions, creating a better flow to the questions.

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

- “invested in threat intelligence” became “used or invested in threat intelligence” (at IDENT) given that some threat intelligence may be accessed without direct payment
- “debriefs to log any lessons learnt” was significantly strengthened to “formal debriefs or discussions to log any lessons learnt” (at INCIDACTION)
- “formally logging incidents” became “keep an internal record of incidents” (at INCIDACTION) to make clearer what was meant by logging.

Furthermore, the following questions received minor amends to the specific language, phrasing or codes used, but are considered to still be broadly comparable to previous years:

- two additional job titles (partner and chair) added to the unprompted list at TITLE
- adding the UK Cyber Security Council as an unprompted information source (INFO)
- “communications and public engagement plans” became “external communications and public engagement plans” (at INCIDCONTENT) to distinguish from internal communications to staff
- “attempt to identify the source of the incident” and “make an assessment of the scale and impact of the incident” at INCIDACTION are both minor updates to previous comparable codes at INCIDCONTENT.

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

- the use of social media accounts (ONLINE) – this activity was considered ubiquitous enough to no longer require tracking
- the use of industrial control systems (ONLINE) – DCMS felt this code tended to underrepresent the use of industrial control systems, which are more commonly found in specific industry sectors, but may not be accurately picked up in an economy-wide business survey
- questions around COVID-19 (COVPRI) and related guidance on home working, video conferencing and moving business online (at SCHEME)
- whether senior management was made aware of the most disruptive breach (BOARDREP).

Cognitive testing

The Ipsos research team carried out 10 cognitive testing interviews with businesses, charities and schools to test comprehension of new or changed questions for 2022.

We recruited all participants by telephone. In previous years, the primary sample source has been organisations that took part in the previous iteration of the survey and gave permission to be recontacted for subsequent research on cyber security over the next 12 months. However, this recontact sample had already been deployed to support DCMS on two other business surveys (the inaugural wave of a longitudinal survey of large organisations and a survey on cyber skills). Therefore, this year Ipsos contracted iThoughts Research to recruit a sample of organisations. We applied recruitment quotas and offered £50 incentive[3] to ensure participation from different-sized organisations across the country, from a range of sectors.

The following lessons emerged from this stage of the research, leading to questionnaire changes:

- We added a brief description of Managed Service Providers (at ONLINE) to avoid confusion and make clear these were not just external cyber security providers.
- We acknowledged that education institutions may find it easier to answer questions on frequency of action (e.g. UPDATE) with reference to school terms or semesters (rather than e.g. “monthly” or “annually”) but opted not to make changes, to maintain consistency across the samples and across years.
- We expanded what was meant by “critical assets” (at MANAGE), so it could clearly be digital as well as physical assets.
- At RULES, we updated the statement on 2FA to make clear this could be for external applications (not just in-house applications) and that it applied even if organisations used 2FA on some applications but not all of them.
- We amended the questions on cyber security strategies (e.g. STRATEGY) to make clear we were referring to formal strategies.
- We agreed at this stage to split the statements on incident management across two questions (INCIDCONTENT and INCIDACTION), splitting out things organisations *had in place* versus what they *had done or planned to do* following an incident.

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 interviewers carried out all the pilot fieldwork between 20 September and 1 October 2021. 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 28 interviews, breaking down as:

- 10 businesses
- 12 charities

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

- 6 schools (4 primary schools and 2 secondary schools).

The pilot sample came from the same sample frames used for the main stage survey (see next section). In total, we randomly selected 550 business leads, 400 charity leads and 320 schools.

The average interview length for the pilot was 23 minutes, which was above target for the main stage (20 minutes). Following feedback from the pilot survey, we amended the survey routing so that several questions (listed here) were only asked of a random half of the sample rather than the full sample, in order to reduce the average interview length. These were chosen on the basis that they were pre-existing questions from previous years – they would not necessarily generate new insights or require the same level of subgroup analysis as new questions – and were not expected to be used in any derived variables (e.g. in relation to the Cyber Essentials or 10 Steps to Cyber Security guidance – see Section 2.7).

- the presence of smart devices and older versions of Windows (at ONLINE)
- having senior management colleagues responsible for cyber security, an external cyber security provider and a business continuity plan covering cyber security (at MANAGE)
- adherence to the following standards or accreditations: ISO 27001, the Payment Card Industry Data Security Standard (PCI DSS) and any National Institute of Standards and Technology (NIST) standards (at COMPLY)
- use of threat intelligence (at IDENT)
- restricting network access to company devices, having separate WiFi networks for staff and visitors, having a Virtual Private Network (VPN) and having an agreed process to follow for phishing emails (at RULES).

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

Following the same approach as last year, the pilot was 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 adding split-sampling to certain questions. Therefore, the 28 pilot interviews were counted as part of the final data.

2.2 Survey microsite and GOV.UK page

As in previous years, a publicly accessible Ipsos microsite (still active as of March 2022) 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 (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 largely matched those included in the all the previous surveys in this series, i.e. private companies or non-profit organisations[4] with more than one person on the payroll. As previously noted, for the first time this year, we included the agriculture, forestry and fishing sector (SIC A).

[4] 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 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 digital 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 VAT-registered 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 primary sample in 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.

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
- 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 6,438 registered charities on the Northern Ireland database, compared to 6,190 in the 2021 survey and 6,118 in the 2020 survey.

Education institutions population and sample frame

The education institutions sample frame came from the following 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:

- 20,809 primary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 5 to 11)
- 4,066 secondary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 11+)
- 309 further education colleges (of which, 4 colleges have closed or merged since the sample was drawn, just before the start of main fieldwork)
- 175 universities.

In order to avoid disclosure, we do not include any information about the specific school type (beyond fitting into the primary or secondary school bracket) in the published data or SPSS file.

Business sample selection

In total, 84,174 businesses were selected from the IDBR for the 2022 survey. This is lower than the 89,372 selected in 2021, although this year's selection includes a greater number of medium and large businesses, reflecting the challenges of surveying these specific groups during the COVID-19 pandemic. In light of three factors, the sample volumes requested have trended substantially upwards since the first Official Statistic survey in this series (Cyber Security Breaches Survey 2017, when 27,948 leads were selected):

- a general trend of declining business survey response rates across the past six years
- an expected shock to contact and cooperation rates as a result of the COVID-19 pandemic and moves to remote or hybrid working
- the highly variable quality of the IDBR sample experienced in recent years (in terms of telephone coverage and 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 2021, 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 2021 report. The boosted sectors included:

- manufacturing (SIC C)
- information and communications (SIC J)
- financial and insurance (SIC K)
- health, social work or social care (SIC Q).

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

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

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

SIC 2007 letter[5]	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
A	Agriculture, forestry or fishing	3,039	57	57	85	3,238
B, C, D, E	Utilities or production (including manufacturing)	2,283	272	159	1,419	4,133
F	Construction	9,625	66	266	300	10,257
G	Retail or wholesale (including vehicle sales and repairs)	4,418	280	731	1,175	6,604
H	Transport or storage	4,038	60	189	360	4,647
I	Food or hospitality	6,457	458	419	611	7,945
J	Information or communications	12,325	485	404	415	13,629
K	Finance or insurance	2,159	605	282	385	3,431
L, N	Administration or real estate	8,685	173	406	1,263	10,527
M	Professional, scientific or technical	7,260	113	479	725	8,577
P	Education	445	30	57	121	653
Q	Health, social care or social work	6,006	315	136	490	6,947
R, S	Entertainment, service or membership organisations	3,109	99	133	245	3,586
	Total	**69,849**	**3,013**	**3,718**	**7,594**	**84,174**

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.

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

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:

- 70,973 of the 84,174 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)
- 3,358 of the 200,203 charities had no valid telephone numbers
- 176 of the 25,359 education institutions had no valid telephone numbers.

We carried out automated telephone tracing (matching the sample frame data to the Dun & Bradstreet database, the DBS Data business 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 was also carrying out another survey with a potentially overlapping sample of businesses and charities – 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:

- 28,923 IDBR records
- 171,533 charities (with exclusions mainly due to the high prevalence of duplicate numbers in this sample frame)
- 18,364 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). An additional opt-in approach was also adopted for the further and higher education populations, which we detail in Section 2.4 (under response rate maximisation).

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 (volumes and as a percentage of originally selected sample)

SIC 2007 letter	Sector description	Micro (1–9 staff)	Small (10-49 staff)	Medium (49–249 staff)	Large (250+ staff)	Total
A	Agriculture, forestry and fishing	552	29	46	72	699
		18%	51%	81%	85%	22%
		829	245	147	1,283	2,504

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)	36%	90%	92%	90%	61%
F	Construction	2,359	57	239	264	2,919
		25%	86%	90%	88%	28%
G	Retail or wholesale (including vehicle sales and repairs)	1,501	224	639	1,028	3,392
		34%	80%	87%	87%	51%
H	Transport or storage	529	49	173	313	1,064
		13%	82%	92%	87%	23%
I	Food or hospitality	2,222	301	337	509	3,369
		34%	66%	80%	83%	42%
J	Information or communications	1,789	339	337	359	2,824
		15%	70%	83%	87%	21%
K	Finance or insurance	1,012	505	251	339	2,107
		47%	83%	89%	88%	61%
L, N	Administration or real estate	1,924	123	344	1,068	3,459
		22%	71%	85%	85%	33%
M	Professional, scientific or technical	1,509	85	409	614	2,617
		21%	75%	85%	85%	31%
P	Education	123	27	46	82	278
		28%	90%	81%	68%	43%
Q	Health, social care or social work	1,468	245	124	413	2,250
		24%	78%	91%	84%	32%
R, S	Entertainment, service or membership organisations	1,060	71	108	202	1,441
		34%	72%	81%	82%	40%
	Total	**16,877**	**2,300**	**3,200**	**6,546**	**29,923**
		24%	**76%**	**86%**	**86%**	**34%**

Sample batches

For businesses and charities, the usable sample for the main stage survey was randomly allocated into batches. The first business batch, excluding pilot sample, had 7,849 randomly selected records. The first charity batch had 1,386 records.

The selection counts were modelled according to two criteria:

- If a particular size band, industry sector or (in the case of charities) income band had a higher interview target based on the disproportionate stratification, we selected more records to reflect that higher target.

- Equally, if a particular size band, industry sector or income band had historically achieved lower response rates, we selected more records to reflect these lower response rate expectations. The response rate expectations were modelled on how other recent DCMS cyber surveys using these same sample frames had performed.

For primary and secondary schools, we selected simple random sample batches of each group. In the first batch, this amounted to 350 primary schools and 600 secondary schools.

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).

Subsequent sample batches were selected according to the same criteria, updated with the remaining interview targets and response rates achieved up to that point. Across all sample groups, seven batches of sample (excluding the pilot batch) 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).

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

- 25,015 IDBR records
- 3,301 charity records
- 1,505 primary schools
- 1,896 secondary schools
- 283 further education colleges
- 171 higher education institutions.

That is to say, we did not use all the available records for businesses, charities, primary schools and secondary schools. The remaining records were held in reserve.

2.4 Fieldwork

Ipsos carried out all main stage fieldwork from 6 October 2021 (following a 2-day pause after the pilot fieldwork) to 21 January 2022 using a Computer-Assisted Telephone Interviewing (CATI) script. This was a similar fieldwork period to the 2021 survey (13 weeks[6]). It is longer than for the 2020 survey (fieldwork across 10 weeks, mainly in 2019, pre-pandemic). It reflects the ongoing 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 2,157 organisations:

- 1,243 businesses
- 424 charities
- 198 primary schools
- 221 secondary schools
- 34 further education colleges
- 37 higher education institutions.

Given the challenges faced during fieldwork this year, these figures are lower than the original interview targets for some groups – we also discuss this in more detail in Section 2.5.

The average interview length was c.22 minutes for all groups.

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

Fieldwork preparation

Prior to fieldwork, the Ipsos research team briefed the telephone interviewing team in a video call, attended by DCMS colleagues. 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 that identified themselves as sole traders with no other employees on the payroll
- organisations that identified themselves as part of the public sector.

In previous years, organisations that claimed to have no computer, website or other online presence were also screened out. This type of ineligibility has dwindled in recent years, and we expect that most organisations making this claim are, in fact, simply refusing to take part by proxy. Therefore, this year, this reason for not taking part was simply listed as a refusal.

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. In practice, our approach exceeded these minimum requirements – any records marked as reaching the maximum number of tries had in fact been called 10 times or more.
- 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:

- The survey had its own web page on GOV.UK and the Ipsos microsite, to let organisations know that the contact from Ipsos 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.

- Interviewers could send a reassurance email to prospective respondents if the respondent requested this. This included a link to the GOV.UK page to confirm the legitimacy of the survey, a link to the relevant Privacy Notice and an option to unsubscribe (by replying to the message and requesting this).
- Ipsos 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 five warm-up and reminder emails across the course of fieldwork to let organisations know that an Ipsos interviewer would attempt to call them, and give them the opportunity to opt in by arranging an appointment. These emails also asked organisations to check the contact details we had for them and to send us better contact details if necessary. They were tailored to the type of organisation, with each email featuring a different subject line and key message to encourage participation.
- 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 and techUK. In practice, this meant that these organisations allowed their identity and logos to be used in the survey introduction and on the microsite, to encourage organisations 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 jointly worked with Jisc and UCISA. These organisations contacted their members, which include IT and cyber security professionals in the further and higher education sectors, to proactively ask them to take part in the survey. Ipsos created a promotional PowerPoint deck explaining the survey to support this. Any opt-in requests were sent via Jisc and UCISA to Ipsos, who set up bespoke calendar appointments with each institution. In total, 2 of the further education interviews and 25 of the higher education interviews were achieved from opt-in requests via these organisations.

Fieldwork monitoring

Ipsos 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

In the 2021 study, as part of a redesigned approach to collecting cost data, we added a new online follow-up survey for businesses and charities (as education institutions did not answer the cost questions). 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 678 respondents were sent this follow-up survey (i.e. they gave their consent), out of the total 775 respondents that were eligible (i.e. had identified breaches or attacks in the telephone survey). Of these, 123 completed the follow-up, representing a response rate of 18 per cent for this online element (vs. 22% last year). Only 6 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 continuing 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, the response rate and the response rate adjusted for unusable or ineligible records, for businesses and charities. The approach for calculating these figures is covered later in this section.

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

Outcome	Businesses	Charities
Total selected from original sample frame	84,174	200,203
Sample without contact details or duplicates post-cleaning	54,251	28,670
Net: total sample with contact details	**29,923**	**171,533**
Sample with contact details left in reserve	4,908	168,232
Net: total sample used (i.e. excluding any left in reserve)	**25,015**	**3,301**
Unresponsive numbers	13,710	4,514
Refusals	4,984	589
Unusable leads with working numbers	3,758	905
Unusable numbers	1,000	159
Ineligible leads – established during screener	215	33
Incomplete interviews	105	33
Net: completed interviews	**1,243**	**424**
Expected eligibility of screened respondents	86%	93%
Response rate	**5%**	**13%**
Response rate adjusted for unusable or ineligible records	**7%**	**20%**

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	Further education	Higher education
Total selected from original sample frame	20,809	4,066	309	175
Sample without contact details or duplicates post-cleaning	5,937	1,025	28	5
Net: total sample with contact details	14,872	3,041	281	170
Sample with contact details left in reserve	13,367	1,896	0	0
Net: total sample used (i.e. excluding any left in reserve)	1,505	1,896	281	170
Incomplete interviews	12	19	03	00
Ineligible leads – established during screener	245	136	00	00
Refusals	176	193	21	15
Unusable leads with working numbers	63	66	16	12
Unusable numbers	32	48	10	05
Unresponsive numbers	779	1,213	198	101
Net: completed interviews	198	221	33	37
Expected eligibility of screened respondents	100%	98%	100%	100%
Response rate	**13%**	**12%**	**12%**	**22%**
Response rate adjusted for unusable or ineligible records	**14%**	**13%**	**13%**	**24%**

Notes on response rate calculations

The following points explain the specific calculations and assumptions involved in coming up with these response rates:

- Response rate = completed interviews / total sample used
- Response rate adjusted for unusable or ineligible records = completed interviews / (completed interviews + incomplete interviews + refusals expected to be eligible + any remaining unresponsive numbers expected to be eligible)
- Refusals exclude excludes “soft” refusals. This is where the respondent was hesitant about taking part, so our interviewers backed away and avoided a definitive refusal.

- Unusable leads with working numbers are where there was communication difficulty making it impossible to carry out the survey (e.g. a bad line, or language difficulty), as well as numbers called 10 or more times over fieldwork without ever being picked up.
- Unusable numbers are 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.
- Unresponsive numbers account for 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.

Original versus revised interview targets

The total achieved interviews for businesses, further education colleges and higher education institutions are under their respective targets set at the outset of the survey. The original targets are laid out in Table 2.5. The targets were intentionally ambitious, and the achieved interviews reflect what was possible in the highly challenging survey environment this year. It should be noted that the differences between the expected margins of error (MoE) at the outset (with the original targets) and the actual margins of error achieved with these sample sizes are, generally speaking, negligible outside of the further education sample.

The margin of error is calculated as the 95% confidence interval, presented here to the nearest whole percentage. That is to say, if we were to conduct this survey 100 times (each time with a different sample of the business population), we would expect the results to be within 2 to 3 percentage points of the results we achieved here in 95 out of those 100 cases.

Table 2.5: Original interview targets and achieved interviews

Sample group	Target	Target MoE[7]	Achieved	Achieved MoE
Businesses	1,400	±2–3 % points	1,243	±2–3 % points
Charities	450	±4–6 % points	424	±4–6 % points
Primary schools	120	±5–9 % points	198	±4–7 % points
Secondary schools	130	±5–9 % points	221	±4–6 % points
Further education	90	±5–9 % points	34	±10–16 % points
Higher education	50	±7–11 % points	37	±9–14 % points

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

The adjusted response rates for all the sampled groups, outside of higher education institutions, were lower than in the 2021 survey. This includes businesses (7%, vs. 19% in 2021), charities (20% vs. 32%), primary schools (14% vs. 37%), secondary schools (13% vs. 25%) and further education colleges (13% vs. 22%).

The lower response rates are likely to be due to a combination of unique circumstances, including:

- the shifting COVID-19 restrictions and associated guidance (particularly for education institutions beginning a new term)

[7] The target margin of error took into account the expected sample stratifications by size and sector (for businesses) and income band (for charities).

- the end of the Coronavirus Job Retention Scheme around the start of fieldwork (on 30 September 2021)
- the attempts by many organisations to move towards hybrid working, which was also disrupted by the emergence of the Omicron variant in late November 2021
- the ongoing challenge of declining response rates in survey fieldwork in general.

While the Cyber Security Breaches Survey 2021 fieldwork also took place under COVID-19 restrictions, the disruption this year appears to have had a more substantial impact on survey performance:

- It was harder to reach organisations via landline numbers given the embedding of video conferencing in working practices.
- 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
- Where we did reach the right person, these individuals were often substantially busier than in previous years due to the overall strain that hybrid working has placed on IT and cyber teams. These teams 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 in 2021 and c.22 minutes this year is also expected to have reduced the response rate – interviewers must mention the average length to respondents when they introduce the survey, and respondents are naturally less inclined to take part in longer interviews.

To a lesser extent, the existence of another DCMS organisational survey on cyber security, the Cyber Security Longitudinal Survey (CSLS), may have impacted the performance of this survey. Ipsos also undertook fieldwork for the CSLS. The CSLS fieldwork took place earlier, between March and July 2021. Organisations that took part in the CSLS were excluded from the sample for the Cyber Security Breaches Survey. However, organisations that were contacted for that survey but opted not to take part may also have been resampled and contacted anew for the Cyber Security Breaches Survey, and been less likely to take part as a result.

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.[8]

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 impacts, 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.

[8] 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).

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 had two business respondents who gave an approximated answer for the COST question (total cost of all breaches or attacks identified in the last 12 months) suggesting an extremely high cost. One these respondents also suggested an extremely high cost for their single most disruptive breach. In one case, we judged their estimate to be legitimate, based on this being a very large business with high revenue (according to Companies House data). The other case was a small business with a low level of net assets (again, according to Companies House data), so we opted to treat this as an outlier, changing their responses to "don't know" at all cost-related questions.[9] The final SPSS data uploaded to the UK Data Archive excludes outlier responses.

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' 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 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.

[9] This includes the following variables in the SPSS data: DAMAGEDIRS, DAMAGEDIRSB, DAMAGEDIRSX, DAMAGEDIRL, DAMAGEDIRLB, DAMAGEDIRLX, DAMAGESTAFF, DAMAGESTAFFB, DAMAGESTAFFX, DAMAGEIND, DAMAGEINDB, DAMAGEINDX, DAMAGE, COSTA, COSTB, COST.

Rim weighting is a standard weighting approach undertaken in business surveys of this nature, because it allows you to weight your sample to represent a wider population using multiple variables. 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 2021.

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 2.6 and Table 2.7 shows the unweighted and weighted profiles of the final data. The percentages are rounded so do not always add to 100 per cent.

Table 2.6: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Micro (1–9 staff)	56%	81%
Small (10–49 staff)	21%	15%
Medium (50–249 staff)	12%	3%
Large (250+ staff)	11%	1%
Sector		
Agriculture, forestry or fishing	3%	4%
Administration or real estate	12%	12%
Construction	9%	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	10%	4%
Information or communications	11%	6%
Professional, scientific or technical	12%	14%
Retail or wholesale (including vehicle sales or repairs	12%	17%
Transport or storage	3%	4%

	Unweighted %	Weighted %
Utilities or production (including manufacturing)	7%	7%

Table 2.7: Unweighted and weighted sample profiles for charity interviews

	Unweighted %	Weighted %
Income band		
£0 to under £10,000	22%	39%
£10,000 to under £100,000	18%	35%
£100,000 to under £500,000	23%	14%
£500,000 to under £5 million	15%	6%
£5 million or more	18%	2%
Unknown income	5%	5%
Country		
England and Wales	89%	84%
Northern Ireland	1%	3%
Scotland	9%	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 (from 2021 to 2018), outside of new questions and deleted questions.

List of changes to old variables in the SPSS file

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

- IDENT5.

The following questions, which were present in the 2021 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 INCIDCONTENT2 variable, we have kept INCIDCONTENT1 rather than delete it). We have then relabelled these variables to make it clear they are no longer being used.

- ONLINE6
- SCHEME6 and SCHEME7
- INCIDCONTENT1, INCIDCONTENT4, INCIDCONTENT5, INCIDCONTENT7, INCIDCONTENT8 and INCIDCONTENT9.

As noted in Section 1.3, the government's 10 Steps to Cyber Security guidance was refreshed between the 2021 and 2022 studies. The overall guidance covers much of the same ground, but the individual 10 Steps have been updated. Consequently, DCMS and Ipsos decided this year to change the way the survey questions are mapped to the 10 Steps. For example, the mapping of the risk management step has been enhanced while the step covering supply chain security is completely new. Given these sorts of changes, it might be considered more challenging for organisations to meet the requirements for the refreshed 10 Steps.

Therefore, the results around the 10 Steps reported in previous years of this study are no longer comparable with the latest results. The final mapping of the 10 Steps to specific survey questions versus the previous mapping is summarised in Table 2.8.

Table 2.8: New and previous mapping of the questionnaire to the 10 Steps to Cyber Security guidance

Step in SPSS	Previous step description and mapping	Current step description and mapping
Step1	Information risk management regime – organisation has formal cyber security policies, and the board are kept updated on actions taken	Risk management – organisation at least annually update senior managers on cyber security actions and have or do at least 2 of the following: ▪ a cyber security policy or strategy ▪ adhere to Cyber Essentials or Cyber Essentials Plus ▪ have undertaken a cyber security risk assessment ▪ have cyber insurance (either a specific or non-specific policy) ▪ have undertaken cyber security vulnerability audits ▪ have an incident response plan ▪ have taken actions to manage the cyber risks from their immediate suppliers or wider supply chain
Step2	Secure configuration – organisation has a policy to apply software updates within 14 days	Engagement and training – staff receive cyber security training, or the organisation has undertaken mock phishing exercises
Step3	Network security – organisation has network firewalls	Asset management – organisations have a list of their critical assets
Step4	Managing user privileges – organisation restricts IT admin and access rights to specific users	Architecture and configuration – organisations have configured firewalls and at least 1 of the following: ▪ secure configurations, i.e. security controls on company devices ▪ a policy around what staff are permitted to do on company devices

Step in SPSS	Previous step description and mapping	Current step description and mapping
Step5	User education and awareness – organisation has a formal policy covering what staff are permitted to do on the organisation's IT devices, and staff receive cyber security training	Vulnerability management – organisations have a patching policy and at least 1 of the following: ▪ have undertaken cyber security vulnerability audits ▪ have undertaken penetration testing ▪ updated anti-malware ▪ a cyber security policy covering Software as a Service (SaaS)
Step6	Incident management – organisation has any incident management processes	Identity and access management – organisations have or do at least 1 of the following: ▪ restrict admin rights to specific users ▪ a password policy ▪ two-factor authentication (2FA)
Step7	Malware protection – organisation has up-to-date malware protection	Data security – organisations have cloud backups or other kinds of backups, and at least 1 of the following: ▪ rules covering secure personal data transfers ▪ a cyber security policy covering removable storage ▪ a cyber security policy covering how to store data
Step8	Monitoring – organisation monitors user activity or uses security monitoring tools	Logging and monitoring – organisations fulfil one of the following criteria: ▪ use security monitoring tools ▪ they have a log of breaches and have had a breach
Step9	Removable media controls – organisation has a formal policy covering what can be stored on removable devices	Incident management – organisations have at least 1 of the following: ▪ an incident response plan ▪ formal debriefs for cyber security incidents
Step10	Home and mobile working – organisation has a formal policy covering remote or mobile working	Supply chain security – organisations have taken actions to manage the cyber risks from their immediate suppliers or wider supply chain

Organisation size variables

There are two organisation size variables, including a numeric variable (SIZEA) and a banded variable (SIZEB). The banded variable in the SPSS does not include the highest band from the questionnaire (1,000 or more employees) because there is no analysis carried out on this group (due to low sample sizes). Instead, it is merged into an overall large business (250 or more employees) size band, which is used across the published report.

Derived cost-related 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. 89% 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 cost 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 combination of all four preceding breach costs, for the single most disruptive breach (damage_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.

Missing data in 1 interview

ID 336572QUIR is a further education college that was mistakenly identified and interviewed as a business (from the IDBR sample). In the post-fieldwork data processing, we recoded this interview to be classified as a further education college. However, because businesses and education institutions do not receive the same questions, this means the following SPSS variables have missing data for this specific interview:

- ONLINE13
- MANAGE2
- COMPLY1
- COMPLY3
- RULES8
- RULES18
- TYPE14

This has no impact on the reported findings.

Missing values

We have treated missing values consistently each year.

- For all non-cost data, only respondents that did not answer a question are treated as missing, and allocated a value of -1. That means that all responses, including “don’t know” (a value of -98) and “refused” responses (-99) are counted in the base and in any descriptive statistics.
- For all cost data, i.e. damagedirs through to cost_bands, the “don’t know” (-98) and “refused” (-99) responses are treated as missing. Practically, this means that any analysis run on these variables systematically excludes “don’t know” and “refused” responses from the base. In other words, this kind of analysis (e.g. analysis to show the mean cost or median cost) only uses the respondents that have given a numeric or banded cost.

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.[10] 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.

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

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.

Chapter 3: Qualitative approach technical details

The qualitative strand of this research focused on businesses, charities and higher education institutions. These same sample groups were included in last year's research. The inclusion of higher education institutions highlights the importance of this group to DCMS, while also acknowledging that the survey sample for this group is inevitably very low – the qualitative strand to explore cyber security approaches in higher education institutions in greater depth.

3.1 Sampling

We took the sample for the 35 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 60-minute interview on the same topic. In total, 891 businesses (72%) and 313 charities (74%) agreed to be recontacted. Of the 37 higher education institutions interviewed, 35 agreed to be recontacted.

Ultimately, we carried out interviews with:

- 19 businesses
- 10 charities
- 6 higher education institutions.

3.2 Recruitment quotas and screening

We carried out recruitment for the qualitative element by email and telephone, using the contact details collected in the survey, and via 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:

- adopted specific cyber security standards or accreditations
- formally reviewed supply chain cyber security risks (including for immediate suppliers and their wider supply chain)
- used or invested in cyber security threat intelligence
- experienced ransomware attacks
- referenced their cyber security risks in a corporate annual report
- taken out an insurance policy specifically covering cyber security
- used Managed Service Providers.

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 research team carried out all fieldwork in December 2021 and January 2022. We conducted the 35 interviews through a mix of telephone and Microsoft Teams calls. Interviews lasted around 60 minutes on average.

DCMS originally laid out their topics of interest for the 2022 study. Ipsos 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:

- decisions around budgeting for cyber security
- board engagement and attitudes
- how organisations aimed to influence the behaviour and culture of staff
- the use and impact of cyber security standards and accreditations
- the decision-making process around supply chain risks
- the use and impact of cyber security threat intelligence
- the approach to information seeking and the impetus to seek out cyber security information and guidance
- approaches to ransomware incidents
- the rationale for reporting cyber security risks in corporate reports
- the use and impact of cyber security insurance
- awareness and understanding around the external reporting of cyber incidents
- any cyber security risks associated with Managed Service Providers.

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 4 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 19 interviewed businesses by size and sector.

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

SIC 2007 letter	Sector description	Total
A	Agriculture, forestry or fishing	0
B, C, D, E	Utilities or production (including manufacturing)	2
F	Construction	3
G	Retail or wholesale (including vehicle sales and repairs)	1
H	Transport or storage	0
I	Food or hospitality	3
J	Information or communications	3

SIC 2007 letter	Sector description	Total
K	Finance or insurance	1
L, N	Administration or real estate	3
M	Professional, scientific or technical	1
P	Education (excluding state education institutions)	5
Q	Health, social care or social work	1
R, S	Entertainment, service or membership organisations	2
	Total	**19**

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)	9
Medium (50–249 staff)	2
Large (250+ staff)	8

Table 3.3 shows a profile of the 10 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	3
£5 million or more	5

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 **2,157 respondents** and the average (mean) survey length was **22 minutes**. Therefore the research compliance cost for the quantitative survey this year was [2,157 × 22 minutes = **791 hours**].
- The qualitative research had **35 respondents** and the average interview length was **60 minutes**. Respondents completed the qualitative interviews in addition to the quantitative survey. The research compliance cost for the qualitative strand this year was [35 × 60 minutes = **35 hours**].

In total, the compliance cost for the Cyber Security Breaches Survey 2022 was **826 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
- split-sampled certain questions – that is to say they were asked to a random half of respondents – to reduce the overall interview length
- offering to carry out interviews at the times convenient for respondents, including evenings and weekends where requested.

The study also adheres to Government Social Research Professional Guidance on ethics.

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)
Partner
Chair

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 S_SAMPTYPE=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_SAMPTYPE=2 OR TYPEX CODE 3: Charity
IF SAMPLE S_SAMPTYPE=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
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 BUSINESS/CHARITY: Personal information about your [IF BUSINESS: customers/IF CHARITY: beneficiaries, service users or donors] held electronically
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: Network-connected devices like TVs, building controls, alarms, speakers etc., sometimes called smart devices
HALF B IF BUSINESS/CHARITY, OR IF EDUCATION: Computers with older versions of Windows installed (e.g. Windows 7 or 8)
A Managed Service Provider, or MSP, that manages a suite of IT services like your network, cloud computing and applications

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

Q9D.COVPRI DELETED PRE-PILOT IN CSBS 2022

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
IF EDUCATION (TYPEXDUM CODE 3): INTERVIEWER NOTE: FOR EDUCATION INSTITUTIONS, "EVERY TERM" MEANS QUARTERLY

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 BUSINESS/CHARITY AND HAVE INSURANCE ((TYPEXDUM CODE 1 OR 2) AND (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)
UK Cyber Security Council

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, CHARITY OR EDUCATION ((SIZEDUM CODES 3–4 AND TYPEXDUM CODE 1) OR TYPEXDUM CODES 2–3): The Cyber Security Board Toolkit
e. IF CHARITY: The Cyber Security Small Charity Guide
f. **DELETED PRE-PILOT IN CSBS 2022**
g. **DELETED PRE-PILOT IN CSBS 2022**

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

ASK IF BUSINESS/CHARITY AND SEEN OR HEARD GOVERNMENT GUIDANCE ((TYPEXDUM CODE 1 OR 2) AND (CYBERAWARE CODE 1 OR ANY SCHEMEa-e 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
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: [IF BUSINESS: Board members/IF CHARITY: Trustees/IF EDUCATION: A governor or senior manager] with responsibility for cyber security
HALF B IF BUSINESS/CHARITY, OR IF EDUCATION: An outsourced provider that manages your cyber security
A formal policy or policies in place covering cyber security risks
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: A Business Continuity Plan that covers cyber security
A written list of the most critical data, systems or assets that your organisation wants to protect

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

ASK ALL
Q29A.COMPLY
((HALF A IF BUSINESS/CHARITY, OR IF EDUCATION) AND IF NOT HEARD OF CYBER ESSENTIALS (SCHEMEa NOT CODE 1)): Does your organisation adhere to the following standard?
(HALF B IF BUSINESS/CHARITY, OR IF EDUCATION) OR IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): Which of the following standards or accreditations, if any, does your organisation adhere to?
READ OUT

MULTICODE
ROTATE LIST BUT KEEP CODES 4 AND 5 TOGETHER
HALF B IF BUSINESS/CHARITY, OR IF EDUCATION: ISO 27001
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: The Payment Card Industry Data Security Standard, or PCI DSS
HALF B IF BUSINESS/CHARITY, OR IF EDUCATION: 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
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: Used or 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)
HALF B IF BUSINESS/CHARITY, OR IF EDUCATION: Only allowing access via company-owned devices
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: 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
HALF B IF BUSINESS/CHARITY, OR IF EDUCATION: A virtual private network, or VPN, for staff connecting remotely
HALF A IF BUSINESS/CHARITY, OR IF EDUCATION: An agreed process for staff to follow when they identify a fraudulent email or malicious website
Any requirement for two-factor authentication when people access your network, or for applications they use

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

Strategy

ASK ALL
Q33D.STRATEGY
Does your organisation have a formal cyber security strategy, i.e. a document that underpins all your policies and processes?

SINGLE CODE
Yes
No
Don't know

ASK IF HAVE A STRATEGY (STRATEGY CODE 1)
Q33E.STRATINT
In the last 12 months, has this strategy been reviewed by your organisation's [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management?

SINGLE CODE
REVERSE SCALE EXCEPT FOR LAST CODE
Yes
No
DO NOT READ OUT: Don't know

ASK IF HAVE A STRATEGY (STRATEGY CODE 1)
Q33F.STRATEXT
Has your cyber security strategy been reviewed by any third parties, such IT or cyber security consultants, or external auditors **at any point**?

SINGLE CODE
Yes
No
Don't know

ASK IF HAVE REVIEWED STRATEGY (STRATEXT CODE 1)
Q33G.STRATREV
Was this a review of your cyber security strategy specifically, or a wider review of your organisation's practices? A wider review might be, for example, when clients carry out due diligence before signing a contract with you.
DO NOT READ OUT

SINGLE CODE
Specific review of cyber security strategy
Part of a wider review of practices
Don't know

Corporate reporting of cyber risks

ASK IF BUSINESS OR CHARITY (BUSINESS/CHARITY (TYPEXDUM CODE 1 OR 2)
Q33H.CORPORATE
This next section is about how cyber security is discussed in any publicly available annual reports of your organisation's activities.

Firstly, did your organisation publish an annual report in the last 12 months?

SINGLE CODE
Yes
No
Don't know

ASK IF HAVE AN ANNUAL REPORT (CORPORATE CODE 1)
Q33I.CORPRISK
Did your latest annual report cover any cyber security risks faced by your organisation?

SINGLE CODE
Yes
No
Don't know

Business standards

Q34.ISO DELETED DURING FIELDWORK IN CSBS 2018

Q35.IMPLEMA DELETED DURING FIELDWORK IN CSBS 2018

Q36.TENSTEPS DELETED PRE-PILOT IN CSBS 2020

Q37.ESSENT DELETED PRE-PILOT IN CSBS 2020

Q38.IMPLEMB DELETED PRE-PILOT IN CSBS 2020

Q39.DELETED PRE-PILOT IN CSBS 2017

Q40.DELETED PRE-PILOT IN CSBS 2017

Q41.DELETED PRE-PILOT IN CSBS 2017

Q42.DELETED PRE-PILOT IN CSBS 2016

Q43.DELETED PRE-PILOT IN CSBS 2016

Supplier standards

Q44.SUPPLY DELETED PRE-PILOT FOR CSBS 2020

Q45.ADHERE DELETED PRE-PILOT FOR CSBS 2020

READ OUT TO 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 BUSINESS OR CHARITY AND REVIEWED ANY SUPPLY CHAIN RISKS (BUSINESS/CHARITY (TYPEXDUM CODE 1 OR 2) AND 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

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 BUSINESS OR CHARITY AND MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (BUSINESS/CHARITY (TYPEXDUM CODE 1 OR 2) AND 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 BUSINESS/CHARITY AND EXPERIENCED ONE TYPE OF BREACH OR ATTACK MORE THAN ONCE ((TYPEXDUM CODE 1 OR 2) AND [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 BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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

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

Q75G.BOARDREP DELETED PRE-PILOT IN CSBS 2022

ASK IF BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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 BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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 BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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 BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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 BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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 BUSINESS/CHARITY AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK ((TYPEXDUM CODE 1 OR 2) AND ([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 BUSINESS/CHARITY AND ANY BREACHES OR ATTACKS ((TYPEXDUM CODE 1 OR 2) AND 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

Incident response

ASK ALL
Q63A.INCIDCONTENT
Which of the following, if any, do you **have in place**, for when you experience a cyber security incident? By this, we mean any breach or attack that requires a response from your organisation.
READ OUT

MULTICODE
ROTATE LIST
Written guidance on who to notify
Roles or responsibilities assigned to specific individuals during or after an incident
External communications and public engagement plans
A formal incident response plan
Guidance around when to report incidents externally, e.g. to regulators or insurers

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

ASK ALL
Q63B.INCIDACTION
IF ANY BREACHES OR ATTACKS (TYPE CODES 1–12): Which of the following, if any, do you **do** when you experience a cyber security incident?
IF NO BREACHES OR ATTACKS (TYPE NOT CODES 1–12): Which of the following, if any, do you **plan to do** if you experience a cyber security incident?
READ OUT

ASK AS A GRID
RANDOMISE LIST

a. Keep an internal record of incidents
b. Attempt to identify the source of the incident
c. Make an assessment of the scale and impact of the incident
d. Formal debriefs or discussions to log any lessons learnt
e. Inform your [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management of the incident
f. Inform a regulator of the incident when required
g. ASK IF HAVE CYBER INSURANCE (CODE 1 OR 2 AT INSUREX): Inform your cyber insurance provider of the incident

SINGLE CODE
Yes
No
DO NOT READ OUT: Don't know
DO NOT READ OUT: Depends on the severity/nature of the incident

ASK ALL
Q63C.RANSOM
In the case of ransomware attacks, does your organisation make it a rule or policy to **not** pay ransomware payments?

SINGLE CODE
Yes
No
Don't know

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 BUSINESS/CHARITY AND ANY BREACHES OR ATTACKS AND NOT REFUSED ALL COST QUESTIONS ((TYPEXDUM CODE 1 OR 2) AND (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.

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 2022?

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

Government guidance for organisations on cyber security

Department for Digital, Culture, Media & Sport

Guidance for organisations just getting started

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

Cyber Aware is the government's advice campaign on how to stay secure online. It covers six essential actions that organisations and their staff should take to make themselves cyber secure.

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data

You can create your own free Cyber Action Plan in under 5 minutes on the Cyber Aware website.

You can also attend a free online training module "Top tips for staff" which takes less than 30 minutes.

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.

Market & Opinion Research International Ltd, Registered in England and Wales No 948470
3 Thomas More Square, London, E1W 1YW
tel: +44 (0)20 3059 5000 | https://www.ipsos-mori.com

Government guidance for organisations on cyber security

Department for Digital, Culture, Media & Sport

Guidance for established businesses and charities including micro and small organisations

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

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

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 46 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. The 10 steps cover:

1. Risk management
2. Staff engagement and training
3. Asset management
4. Security architecture and secure configurations
5. Vulnerability management
6. Identity and access management
7. Data security
8. Logging and monitoring
9. Incident management
10. Supply chain security

Appendix C: Topic guide

Introduction (FOR ALL)

- Thank participant for taking part; introduce self and Ipsos
- **Explain the project:** we are exploring some topics about cyber security from the survey in more depth on behalf of DCMS
- All responses are confidential and anonymous
- **Recording:** get permission to digitally record
- **Length:** approximately 60 mins

GDPR added consent (once the recorder is on)

Ipsos' legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview.

Can I check that you are happy to proceed?

Perception of cyber security risk (ASK ALL)

SKIP IF THEY ARE PRESSED FOR TIME

- Briefly, what would you say are the top 2-3 cyber security priorities for your organisation right now?

Cyber security decision-making – part A (ASK ALL)

Budget decisions

- How does your organisation budget for cyber security? Who decides the budget? How frequently is it reviewed? PROBE:
    - How proactive/reactive are spending decisions? How much is in response to incidents? How much of it is planned?
    - Is it cyber security -specific, or part of a wider team budget (e.g. IT)? How well does cyber security get prioritised within this wider budget?
    - What do you need to do to justify any spending (e.g. a business case)? How easy is it to produce this?
- Are any areas of cyber security hampered by budget constraints? If you had extra money right now for cyber security, where would it go?
- How has spending changed over the last few years? Has it trended upwards/downwards? What has driven this?

Board engagement and attitudes

- How closely are board members (directors, trustees etc.) and your executive team (CEOs etc.) involved in cyber security decisions? PROBE INVOLVEMENT IN:
    - Deciding what your cyber security priorities/critical assets are
    - Spending decisions (including staffing and outsourcing)
    - Incident response
- How well do board members/executive team understand your organisation's cyber security needs? How well do they understand your approach? PROBE:
    - What bits do they understanding well/less well? What further support would you want to see from them on cyber security?
    - What implications does this have for your cyber resilience? How much does it matter if board members are engaged or not?
    - What training, if any, have they had in cyber security? How was this delivered? How effective was it?
    - What do you think other organisations like yours could learn from the way your board or executive team approaches cyber security?

SKIP IF LACKING TIME: *Before this interview, we sent you a link to the Cyber Security Board Toolkit on the National Cyber Security Centre's website: https://www.ncsc.gov.uk/collection/board-toolkit*

- Had you used this toolkit before? IF YES, THEN ASK ABOUT THEIR EXPERIENCE, OTHERWISE PROBE:
    - How would your board respond to this toolkit?
    - Which bits are most useful? What could be improved?

Embedding culture/behaviour change

- Across your wider staff, how do you go about embedding good behaviour and practice when it comes to cyber security? What is most effective? PROBE RELATIVE IMPORTANCE OF:
    - Monitoring of staff
    - Relationships between staff and cyber/IT teams
    - Awareness raising and training (any good examples)?
    - Exercises and feedback
- How prepared would you say your wider staff are for a major cyberattack or cyber incident, if it took place tomorrow?
- What's the biggest challenge in this area? What do you find hard? PROBE:
    - Willingness/pushback from staff
    - Skills of staff/senior management
    - Hybrid working

- Budgets/training budgets

Cyber security decision-making – part B (EVERYONE IS ELIGIBLE FOR ONE SUBSECTION, LISTED IN THE SAMPLE PROFILE)

Standards and accreditation decisions (IF HAVE ACCREDITATIONS)

- Tell us about the external cyber security standards and accreditations your organisation has adopted.
    - What made you decide to apply for this? PROBE: internal pressure (e.g. board members), external pressure/requirements from clients, investors, insurance providers etc., for branding/marketing
    - What made you choose this standard over others? PROBE: ISO 27001, Cyber Essentials, Cyber Essentials Plus
    - What involvement did your board/executive team have in this? How well do they understand this standard and what it means?
    - How has this standard improved your cyber security? What changes did you have to make to meet this standard, if any?
- Have your cyber security standards and accreditations helped you win contracts or new business?
- Have you heard of the NCSC's Cyber Assessment Framework? Have you used this in your organisation? What has your experience been?

Supply chain decisions (IF HAVE SUPPLY CHAIN MANAGEMENT)

- How do you go about managing cyber security risks from your wider supply chains? How systematic/formalised is this process?
- Who is responsible? How engaged are your board/executive team in this?
- How would you rate your awareness/monitoring of the risks? PROBE: Do you know which suppliers have access to your IT systems? Which ones are essential to your continuity of production/service?
- How often do you talk to your suppliers about cyber security? How do you ensure they are aware of their responsibilities?
- How would you react to suppliers if they had cyber security incidents affecting you? Would you expect to provide any support?
- Has anything changed in terms of how you look at cyber security risks from your supply chains in the last 2 years? Has it got any more/less important?

Threat intelligence decisions (IF USE THREAT INTELLIGENCE)

- How has your organisation used cyber threat intelligence?
    - Was this a one-off or an ongoing investment in threat intelligence? How often do you review it?

- What was behind your decision to invest in threat intelligence?
- What impact does this have on your approach to cyber security?
- What knowledge does your board/executive team have of this threat intelligence? Are they informed about it? Does it influence their decisions?

Information seeking (ASK ALL)

- How regularly would you typically seek out information and guidance around cyber security? Do you have any go-to sources?
- Can you tell me about any specific instances in the last 2 years when you have sought external information or guidance around cyber security, or done your own research into any aspect of it?
- Have you ever sought cyber security information or guidance in response to:
    - Media/news stories about cyber security
    - Your own cyber security breaches/incidents
    - Interest/enquiries from the board/executive team/other staff
- Where did you look in these specific cases? What kind of information or guidance did you find? What was the source?
- How easy was it to find the kind of information or guidance you needed?
- What did you do/implement based on the information you found?
    - Did you discuss the information with anyone else in the organisation?
    - Did you enact anything? Make any changes to processes or technical controls?

Ransomware (ASK ALL)

Ransomware risk management

- How much of a threat would you say ransomware is to your organisation? How does this compare to other types of cyber security breaches?
- Has the importance of ransomware changed over time for your organisation?
- What level of knowledge would you say you have in this area? What have you seen or heard about it?
- How does your organisation protect itself against ransomware and it effects?

Ransomware incident response

IF NOT HAD RANSOMWARE BEFORE:

- Do you have a policy around ransomware, if you ever had a ransomware attack? What did you base this on?
- Talk me through what would happen if you experienced a ransomware attack tomorrow? PROBE:

- What steps would there be in your response?
- Who would be alerted? Who would you report it to externally, if anyone? What would encourage/prevent you to report it?

- Do you have a rule to pay out/not pay out after a ransomware attack? Tell me about the decision-making behind this.
  - What involvement does your board/executive team have in this decision?

IF HAD RANSOMWARE:

In the survey you said that your organisation experienced a ransomware attack in the last 12 months.

- Talk me through what happened. PROBE:
  - The steps you took in response – did this follow an existing plan? Have you developed/updated a response plan since then?
  - Who was alerted? Did you report it externally? What was behind this decision? What would have encouraged/prevented you to report it?
  - IF YES: How did you go about reporting it?
  - Did you pay out? Tell me about the decision-making behind this.
  - What was the impact? What happened to your data? Was there a financial impact? How did it affect staff (e.g. causing stress)?
  - Have you made changes to policies or processes as a result?
- What would you do differently/quicker, if anything, if this happened again?

Corporate annual reporting of cyber security issues (ON ROTATION, LISTED IN THE SAMPLE PROFILE)

In the survey you said that your organisation included a section on your cyber security risks in your last annual report.

- What is the main purpose of this section? Who is the intended audience?
- Could you outline the content of this section? What information was included? PROBE:
  - Strategy, risk assessments, governance arrangements, technical settings, training, supply chains, incidents
  - Would you typically exclude any of these areas? What's the rationale behind that?
- How is this section compiled and edited? PROBE:
  - Who writes it? Who decides on content and focus? Who approves it?
  - How much involvement does the board/executive team have over this section of the report? How much is left to the cyber/IT team alone?
  - Was the cyber security content compiled and edited in the same way as the rest of the document or differently? How/why?

- How does this reporting compare to your competitors/others in your sector? Would you consider your organisation behind or ahead of others in terms of what you publish?

Cyber security insurance (ON ROTATION, LISTED IN THE SAMPLE PROFILE)

In the survey you said that your organisation has an insurance policy specifically covering cyber security.

- Could you describe to me the key elements of the policy? Which aspects are the most important for your organisation? PROBE:
    - coverage of specific events/incidents (e.g. ransomware)
    - any post-incident support (e.g. incident management, communications management, forensic analysis)
    - any ongoing guidance/support outside of incidents
- Are any types of cyber security breaches not covered?
- Does the policy cover any third parties (e.g. clients, suppliers)?
    - How important is this? Was it an active consideration when you took out the policy?
- What kind of real-life situation would there need to be for you to claim through this policy?
    - How likely do you think you are to claim through it within the next few years?
    - Are there any types of incident where you wouldn't claim/inform your insurer, even if they are covered? What would be the rationale?
- How has the insurance affected your approach to cyber security?
    - Have you had to make any changes/maintain any standards to meet the insurer's requirements? What impact has this had?

External reporting of breaches (ON ROTATION, LISTED IN THE SAMPLE PROFILE)

- What kinds of cyber security incidents/circumstances would lead to you alerting any of the following bodies or groups:
    - A regulator
    - Your bank or insurance company
    - The police or a related body like Action Fraud – what kinds of breaches do you think they are interested in hearing about?
    - The National Cyber Security Centre – what kinds of breaches do you think they are interested in hearing about?
    - Your customers, investors or suppliers
- Have you previously reported breaches to any of these groups? IF YES: Please talk me through the breach and the decision behind reporting it.

- Do you have a policy or rules around external reporting of breaches? E.g. do you report breaches as a matter of course? What's the reason for this?
- Have you ever had a serious breach you didn't report to anyone externally? IF YES: Please talk me through the breach and why you didn't report it.
- What do you think the benefits are of reporting breaches externally? And what are the drawbacks/costs of doing so?
- Do you think other organisations in your sector take the same approach?

Managed Service Providers (ON ROTATION, LISTED IN THE SAMPLE PROFILE)

This last section is about Managed Service Providers, or MSPs, that manages a suite of IT services like your network, cloud computing and applications. In the survey, you said your organisation used one or more MSPs.

- What does your MSP(s) provide? Is it a software package or a service? How essential are they to your continuity of production/service?
- What were the factors involved in choosing your MSP(s)?
    - Was cyber security one of the considerations? IF YES: How much of a priority would you say this was compared to other factors (e.g. price, reliability, word of mouth)?
- How much of a risk do you think your MSP(s) poses to your organisation's cyber security?
    - Have you discussed this with them? How willing are they to discuss it/share information on their cyber security?
    - Does your contract with your MSP say anything about cyber security? What's covered?
    - Who is responsible for cyber security between them and you, when it comes to their service? E.g. for incident response?

Summary & wrap-up

- Thinking about all the challenges we talked about, are there any areas that you think your organisation could improve on, or could focus on more?
- What's the most important thing you think we have talked about?

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.

    - Alice Stratton, Ipsos
    - Harry Williams, Ipsos
    - Eleanor Myles, Ipsos
    - Nick Coleman, Ipsos
    - Jayesh Navin Shah, Ipsos.

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 Maddy Ell. The responsible statistician is Robbie Galluci. For enquiries on this release, from an official statistics perspective, please contact DCMS 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 Terms and Conditions which can be found at https://ipsos.uk/terms.

Department for Digital, Culture, Media & Sport

4th Floor
100 Parliament Street
London
SW1A 2BQ