



Cyber Security Longitudinal Survey Wave 1

Technical Annex

This Technical Annex provides details of the methodology of the Cyber Security Longitudinal Survey (CSLS) Wave 1. It covers the quantitative survey (pilot fieldwork carried out between March – April 2021, main fieldwork April – July 2021) and qualitative element (carried out in July-August 2021), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

This annex supplements a [main Statistical Release](#) and [infographic summaries](#) published by the Department for Digital, Culture, Media and Sport (DCMS), covering the results for businesses and charities.

The Cyber Security Longitudinal Survey (CSLS) is a three-year longitudinal study, which follows the same organisations over time. It aims to better understand cyber security policies and processes within medium and large businesses and high-income charities, and the extent to which these change and improve over time.

It will also explore the links over time between these policies and processes and the likelihood and impact of a cyber incident to quantify specific actions resulting in improved cyber incident outcomes.

This is the first research year, and therefore the main objective of this report is to establish a baseline of findings. The quantitative survey was carried out in March-July 2021 and the qualitative element in July-August 2021.

Responsible analyst:

Maddy Ell

Responsible statistician:

Robbie Gallucci

Statistical enquiries:

evidence@dcms.gov.uk

General enquiries:

enquiries@dcms.gov.uk

Media enquiries:

020 7211 2210

Table of Contents

- Chapter 1: Overview 3**
 - 1.1 Summary of methodology 3
 - 1.2 Difference from the Cyber Security Breaches Survey 3
 - 1.3 Benefits and limitations of the survey 5
- Chapter 2: Survey approach and technical details 7**
 - 2.1 Survey and questionnaire development 7
 - 2.2 GOV.UK page 10
 - 2.3 Sampling 10
 - 2.4 Fieldwork 16
 - 2.5 Fieldwork outcomes and response rate 18
 - 2.6 Data processing and weighting 19
 - 2.7 SPSS data uploaded to UK Data Archive 21
- Chapter 3: Qualitative approach technical details 25**
 - 3.1 Sampling 25
 - 3.2 Recruitment quotas and screening 25
 - 3.3 Analysis 26
- Chapter 4: Research burden 27**
- Appendix A: Questionnaire 28**
- Appendix B: Topic guide 48**
- Appendix C: Further information 56**

Chapter 1: Overview

1.1 Summary of methodology

The Cyber Security Longitudinal Survey (CSLS) Wave 1 is year one of a three-year longitudinal research project. For this study:

- we undertook a random probability multimode (telephone and online) survey of 1,205 UK businesses and 536 UK registered charities. The pilot survey took place between 9th March and 6th April 2021, the main stage survey took place between 27th April and 15th July 2021. The data for businesses and charities have been weighted to be statistically representative of these two populations
- we carried out 30 in-depth interviews in July-August 2021 to gain further qualitative insights from some of the organisations that answered the survey

For years two and three of the three-year study, data will be collected using a refreshed panel design. This means that we will largely interview the same organisations as in year one, but during year two and three we will also use some top-up sample. Therefore, we will focus the study on repeat observations with the same organisations where possible and replace any drop-outs from the survey with fresh sample using additional leads. This not only allows for better cross-sectional analysis, as it ensures a representative sample overall each wave, but also adds flexibility to the longitudinal analysis as there is no hard requirement for organisations to take part in all three waves.

This design will enable delivering the following key long-term objectives of this research:

- explore how and why UK organisations are changing their cyber security profile and how they implement, measure and improve their cyber defences
- provide a more in-depth picture of larger organisations, covering topics that are lightly covered in the Cyber Security Breaches Survey (CSBS), such as corporate governance, supply chain risk management, internal and external reporting, cyber strategy, cyber insurance, and ransomware
- in following waves, explore the effect of actions adopted by organisations to improve their Cyber Security to likelihood and impact of a cyber security incident

The scope of this survey are medium (defined as 50-249 employees) and large (defined as 250+ employees) businesses and large charities (defined as a turnover of at least £1million).

Businesses with less than 50 employees, charities with a turnover smaller than £1 million, and all public-sector organisations were outside the scope of the survey. In addition, businesses with no IT capacity or online presence were deemed ineligible, which led to a small number of specific sectors (agriculture, forestry, and fishing) being excluded.

1.2 Difference from the Cyber Security Breaches Survey

The results from this study are entirely independent from the Cyber Security Breaches Survey (CSBS), which is an annual study of UK businesses, charities and education institutions as part of the National Cyber Security Strategy. This study differs from the CSBS in several important respects. First, it uses a longitudinal design to better identify drivers for change in cyber security whereas the CSBS uses a cross-sectional sample to provide a static view of cyber resilience. Second, this survey focuses only on medium and large businesses and high-income charities whereas the CSBS includes all businesses (micro, small, medium, and large), all income

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

charities and educational institutions. Additionally, while there are some similarities in the questions and topics covered by the two surveys, results are not comparable.

The CSBS is an official government statistic, and representative of all UK businesses, charities, and educational institutions. Therefore, for overall statistics on cyber security, results from CSBS should be used. Overlapping questions where data from CSBS should be used include:

Question ID	Question wording
Q_INSUREX	There are general insurance policies that provide cover for cyber security incidents, among other things. There are also specific insurance policies that are solely for this purpose. Which of the following best describes your situation?
Q_COMPLY	Which of the following standards or accreditations, if any, does your organisation adhere to?
Q_IDENT	Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation?
Q_RULES	And which of the following rules or controls, if any, do you have in place?
Q_TRAINED	In the last 12 months, have you carried out any cyber security training or awareness raising sessions specifically for any [IF BUSINESS: staff/IF CHARITY: staff or volunteers] who are not directly involved in cyber security?
Q_SUPPLYRISK	In the last 12 months, has your organisation carried out any work to formally assess or manage the potential cyber security risks presented by any of these suppliers [IF CHARITY: or partners]?
Q_INCIDENT	Have any of the following happened to your organisation in the last 12 months?
Q_DISRUPT	What kind of incident was this?
Q_OUTCOME	Thinking of all the cyber security incidents experienced in the last 12 months, which, if any, of the following happened as a result?
Q_IMPACT	And have any of these incidents impacted your organisation in any of the following ways?
Q_RESTORE	How long, if any time at all, did it take to restore business operations back to normal after the incident was identified? Was it...?
All questions related to incident costs:	
Q_DAMAGEDIRS / Q_DAMAGEDIRS B	External payments made when the incident was being dealt with
Q_DAMAGEDIRL / Q_DAMAGEDIRLB	External payments made in the aftermath of the incident
Q_DAMAGESTAFF / Q_DAMAGESTAFFB	Cost of the staff time dealing with the incident
Q_DAMAGEIND / Q_DAMAGEINDB	Value of any damage or disruption during the incident
Q_COSTA/B	Financial cost of all the cyber security incidents experienced in the last 12 months

To see publications of the Cyber Security Breaches Survey, please visit the gov.uk website¹.

¹ <https://www.gov.uk/government/collections/cyber-security-breaches-survey>

1.3 Benefits 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:

- covering several countries alongside the UK (mainly US-based studies), which leads to a small sample size of UK organisations
- conducted by private sector firms with the objective of selling their cyber consult
- using partially representative sampling or online-only data collection methods
- most surveys are one-off or ‘cross sectional’, giving a snapshot at a point in time

By contrast, the Cyber Security Longitudinal Survey is intended to be statistically representative of medium and large UK businesses and all relevant sectors, and of high-income UK registered charities.

The main benefits of the Cyber Security Longitudinal Survey are:

- the use of random probability sampling to avoid selection bias
- multimode survey including a telephone data collection approach, which aims to also include businesses and charities with less of an online presence (compared to online surveys)
- a comprehensive attempt to obtain accurate spending and cost data from respondents, giving respondents flexibility in how they can answer (e.g., allowing numeric and banded £ amounts), and sending them a follow-up online survey to validate answers given in telephone interviews
- a consideration of the cost of cyber security incidents 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)
- by being a three-year longitudinal study, data will be collected from the same unit (in this case businesses or charities) on more than one occasion to enable analysing the link between large and medium organisations’ cyber security behaviours and the extent to which they influence the impact and likelihood of experiencing an incident over time

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:

- the longitudinal research method introduces the risk of sample attrition. The dropout rate is expected to be fairly low with most organisations taking part indicating they are happy to participate in future years. Dropout is largely unavoidable, and the figure should be disclosed in future years
- organisations can only tell us about the cyber security incidents that they have detected. There may be other incidents affecting organisations that are not identified as such by their systems or by staff, such as viruses or other malicious code that has so far gone unnoticed. Therefore, the survey may have a tendency to systematically underestimate the real level of incidents

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

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

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

Ipsos MORI developed the questionnaire and all other survey instruments (e.g., the interview script and briefing materials) and DCMS had final approval of the questionnaire. The development of the survey took place over three stages from January to March 2021:

- stakeholder engagement, including a virtual workshop with industry and government representatives
- cognitive testing interviews with 15 organisations (8 businesses and 7 charities)
- a pilot survey, consisting of 140 interviews (84 businesses and 56 charities)

Stakeholder engagement and initial questionnaire review (including academic input)

Steven Furnell, Professor of Cyber Security from the University of Nottingham, was involved as an academic consultant in the survey development. As part of the initial questionnaire review, Professor Furnell engaged with academic colleagues from various UK universities in January-February 2021 to seek feedback on suggested topics to cover. He also carried out his own review of the questionnaire.

Additionally, Ipsos MORI held a virtual workshop with government and industry stakeholders in January 2021. The aim of the workshop was to review suggested topics, to collect feedback on any research gaps, and to identify and discuss emerging trends in cyber security that are specific to large organisations that we would want to cover in our baseline year.

The workshop was attended by industry stakeholders from organisations such as: the Association of British Insurers (ABI), the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), the Institute of Risk Management, TechUK and the Institute of Chartered Accountants in England and Wales (ICAEW). Government stakeholders included: the Home Office, the Charity Commission, the Scottish Government, the National Crime Agency, and the National Cyber Security Centre (NCSC).

Based on these discussions, the feedback from stakeholders, and their own internal thinking, DCMS agreed the following question/topic areas to be covered in the questionnaire:

- cyber profile of organisations
- board involvement in cyber security
- current cyber security policies and processes and any improvements made over the last 12 months
- cyber incident management
- supplier risks
- influencers of changes in policies and processes
- use and forms of cyber insurance
- sources of information organisations are aware of / use on cyber security
- prevalence and impact of incidents

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

Cognitive testing

The Ipsos MORI research team carried out 15 cognitive testing interviews with businesses and charities to test comprehension questions.

We recruited all participants by telephone. We looked to recruit organisations that had taken part in the 2020 Cyber Security Breaches Survey and had given permission for recontact. We applied recruitment quotas and offered £50 incentive² to ensure participation from different-sized organisations across the country from a range of sectors or charitable areas.

After this stage, the questionnaire was shortened and required some minor tweaks to ensure that the questions were concise, clear, and relevant to your key respondent groups.

Pilot survey

The pilot survey was used to:

- test the questionnaire CATI (computer-assisted telephone interviewing) script
- time the questionnaire
- test the usefulness of the interviewer briefing materials
- test the quality and eligibility of the sample (by calculating the proportion of the dialled sample that ended up containing usable leads)

Ipsos MORI interviewers carried out all the pilot fieldwork between 9th March and 6th April 2021. Again, we applied quotas to ensure the pilot covered different-sized businesses from a range of sectors, and charities from different countries. We carried out 140 interviews, breaking down into:

- 84 businesses
- 56 charities

The pilot sample came from the same sample frames used for the main stage survey (see next section). In total, we randomly selected 1500 business leads and 300 charity leads.

The questionnaire length for the pilot was 25 minutes, which was above target for the main stage. Therefore, we made some changes to the questionnaire by:

- removing three statements from Q_ONLINE (a question that asks whether the organisation currently uses or provides various online services)
 - video conferencing software such as Teams or Zoom
 - network-connected devices like TVs, building controls, alarms, speakers etc. sometimes called smart devices
 - computers with older versions of Windows installed (i.e., Windows XP, 7 or 8)
- removing a question on what proportion of staff accessed the organisation's network or files from the organisation's own workplace, from home or from another location on a typical working day in the past month
- removing one statement from Q_IDENT (a question that asks about any actions taken to identify risks): 'Any other actions to identify risks'

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

- removing four statements from Q_IMPROVE (a question that asks respondents whether they have improved or expanded aspects of their cyber security)
 - any policies or processes for removable devices (e.g., USB sticks)
 - any cyber security awareness raising or training activities for staff (was asked only of respondents who provide staff training)
 - any processes for managing cyber security risks from suppliers /or partners (was asked only of respondents who manage supplier risks)
 - the team you have working on cyber security
- removing a question asking what is provided under the organisation's insurance policy (if they have one)
- removing a question on the maximum amount, in pounds, that organisations are covered for under their insurance policy (if they have one)
- removing two statements from Q_BOARDENGAGE (a question on the way board members engage with cyber risks)
 - the board challenges the cyber risk information it receives
 - the board is enabled to make decisions to adapt the cyber risk profile
- removing seven statements from Q_INCIDCONTENT (a question asking about what is covered in the organisation's written incident management processes)
 - guidance on who to notify within your organisation
 - how to document and track incidents
 - roles or responsibilities assigned to specific individuals during or after an incident
 - a process to identify the source of the incident
 - a process to assess the severity of the incident
 - a process to categorise the type of incident
 - a post-incident review process

We also decided to remove all 'Other, please specify' open response options throughout the survey. This is because during the pilot stage we received a very low proportion of responses to these, suggesting that the existing pre-codes cover most possible scenarios we would like to measure.

The validation survey, which was an additional online survey to confirm responses given for any questions that required a numerical response (e.g., the cost implications of cyber incidents) was also removed after the pilot stage. This was done for various reasons, firstly to shorten the survey due to low uptake. Secondly, close to all results matched up to answers given during telephone interviews, suggesting that respondents were able to provide accurate information over the phone.

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

The pilot was also used as a soft launch of the main fieldwork. We used the same sample frames for the main stage. The sample selection and interviewing process for the pilot was random. Moreover, there were no substantial post-pilot changes other than cuts to the questionnaire. Therefore, the 140 pilot interviews were included as part of the final data.

2.2 GOV.UK page

A [GOV.UK page](#) was used to provide reassurance that the survey was legitimate and provide more information before respondents agreed to take part.

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

2.3 Sampling

Business population and sample frame

The target population of this research are medium and large businesses. This is due to these businesses being more likely than smaller businesses to have specialist staff dealing with cyber security and to have formal policies and processes covering cyber security risks. Additionally, according to the feasibility study conducted prior to this research, similar proportions of medium and large businesses experienced cyber security incidents within the last 12 months, both of which report a higher rate than smaller organisations. Therefore, medium and large businesses provide the most insight into how UK organisations are currently managing their Cyber Security.

Medium and large businesses were defined as:

- medium businesses with 50-249 employees (a population³ of 36,140 according to the latest BEIS Business Population Estimates⁴)
- large businesses with 250+ staff (a population of 7,835, with 3,845 being very large with 500+ staff according to the latest BEIS Business Population Estimates)

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

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

Exclusions from the IDBR sample

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

In line with the approach taken by other previous Ipsos MORI surveys on cyber security, organisations in the agriculture, forestry and fishing sectors (SIC 2007 category A) were also excluded. There are practical considerations that make it challenging to interview organisations in this relatively small sector, as this requires additional authorisation from the Department for Environment, Food and Rural Affairs if sampling from the IDBR. We also judged cyber security

³ Population figures cited for medium businesses and large businesses refer to the official estimates of the total number of private sector businesses in the UK

⁴ See <https://www.gov.uk/government/statistics/business-population-estimates-2020>.

to be a less relevant topic for these organisations, given their relative lack of e-commerce. This exclusion will be reviewed annually by DCMS.

Charity population and sample frames (including limitations)

The target population of charities was high-income charities with £1 million or more in annual income (a population of 9,333 across the three UK charity regulator databases).

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 it 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 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 a truly random sample of Northern Ireland charities at present.

The following exclusions were also made from the above-mentioned three sample sources:

- no valid telephone number
- where the telephone number appeared for another charity
- schools, colleges, or universities (which are also registered charities)

Business sample selection

In total, 47,859 businesses were selected from the IDBR for the survey.

We determined this to be an accurate sample size based on experiences on the Cyber Security Breaches Survey. Challenges considered were to mitigate against the risk of varying sample quality experienced in recent years (in terms of telephone coverage and usable leads), as well as the anticipated difficulty in reaching businesses during the COVID-19 pandemic. We wanted to ensure that there was enough reserve sample to meet the size-by-sector survey targets.

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 large and very large businesses from the selected sample, and, without such stratification, we would expect 82% of a random non-small business sample to be medium businesses. Hence, the sample of large

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

and very large businesses was boosted relative to medium businesses. Both the large and very large groups are broadly equal in size, so neither needed to be boosted relative to the other.

Following the approach taken by previous cyber security research conducted by Ipsos MORI, we also boosted specific sectors that tend to be more engaged with cyber security within the medium business sample. This was done to improve the statistical reliability of the estimates since more engaged businesses tend to adopt a greater range of cyber security behaviours – a greater variance in responses leads to lower standard errors. The boosted sectors included:

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

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

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

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

SIC 2007 letter	Sector Description	Medium (50 to 249 staff)	Large (250 to 499 staff)	Very large (500 or more staff)	Total
B, D, E	Utilities or production	378	63	72	513
C	Manufacturing	6,347	776	553	7,676
F	Construction	2,134	174	138	2,446
G	Retail or wholesale (including vehicle sales and repairs)	5,145	571	604	6,320
H	Transport or storage	1,568	169	197	1,934
I	Food or hospitality	3,093	313	336	3,742
J	Information or communication	2,150	223	204	2,577
K	Finance or insurance	1,007	170	222	1,399
N	Administration	4,146	578	563	5,287
L	Real estate	564	93	117	774
M	Professional, scientific or technical	3,880	374	363	4,617
P	Education (excluding public sector schools, colleges and universities)	1,510	320	342	2,172
Q	Health, social care or social work (excluding NHS)	5,099	483	408	5,990
R	Arts or recreation	1,222	179	140	1,541
S	Service or membership organisations	751	69	51	871
Total		38,994	4,555	4,310	47,859

Charity sample selection

The charity sample was treated as a simple random sample. This was due to it not being feasible to boost very high-income bands (e.g., the £5 million+ or £10 million+ bands) as a result of the relatively low population sizes. The only other reliable variable on the sample is country, which followed the same logic as regional stratification for businesses.

Sample telephone tracing and cleaning

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

Not all the original sample was usable. In total:

- 4,190 of the 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)
- 182 of the charities had no valid telephone numbers
- 4,639 records were excluded due to being duplicates (3,653 businesses and 986 charities)
- 5,094 charity records were excluded due to having an income less than £1 million
- 423 charity records were excluded as these were colleges or universities that are also registered charities
- 39 records were excluded as do not contact

Table 2.2 breaks the usable business leads down by size and sector.

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

SIC 2007 letter	Sector Description	Medium (50 to 249 staff)	Large (250 to 499 staff)	Very large (500 + staff)	Total
B, D, E	Utilities or production	339	49	63	451
C	Manufacturing	5,894	689	493	7,076
F	Construction	1,956	149	118	2,223
G	Retail or wholesale (including vehicle sales and repairs)	4,605	502	526	5,633
H	Transport or storage	1,421	151	173	1,745
I	Food or hospitality	2,429	263	286	2,978
J	Information or communication	1,774	185	166	2,125
K	Finance or insurance	896	151	187	1,234
N	Administration	3,435	490	475	4,400
L	Real estate	468	76	98	642
M	Professional, scientific or technical	3,292	309	293	3,894
P	Education (excluding public sector schools, colleges and universities)	938	229	301	1,468
Q	Health, social care or social work (excluding NHS)	3,694	322	277	4,293
R	Arts or recreation	912	132	108	1,152
S	Service or membership organisations	526	56	39	621
Total		32,579	3,753	3,603	39,935

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

Sample batches

For businesses and charities, the usable sample for the main stage survey was randomly allocated into separate batches. The first business batch, excluding the pilot sample, had 11,375 records proportionately selected to incorporate sample targets by sector band. These were then disproportionately stratified to include more large and very large businesses owing to both the expected difficulty in contacting these businesses and to the response rates by sector and size band. In other words, more sample was selected in sectors and size bands where there was a higher target or where response rates had been relatively low in recent fieldwork on the Cyber Security Breaches Survey (2020 and 2021). The first charity batch had 1,823 records selected.

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

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

- 7,848 IDBR records
- 1,405 charity records

Across all sample groups, four batches of sample (including 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).

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

2.4 Fieldwork

Ipsos MORI carried out main stage fieldwork between 27th April and 15th July 2021 using a Computer-Assisted Telephone Interviewing (CATI) and an online script.

In total, we completed interviews with:

- 1,205 businesses
- 536 charities

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

Fieldwork preparation

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

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

Screening of respondents

Interviewers screened all sampled organisations at the beginning of the call to identify the right individual to take part and to ensure the business was eligible for the survey. At this point, the following organisations would have been removed as ineligible:

- businesses with less than 50 employees
- charities with an income under £1 million

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.

All business sample contacts were asked to confirm whether (or not) they were a registered charity. Those saying 'yes' (and who subsequently confirmed that their annual income was over £1 million) were included as charities and asked the survey questions on this basis. In total, 86 organisations who were originally included in the business sample confirmed that they were registered charities. Post-fieldwork checks were then conducted to also verify the nature of these organisations.

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.

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

Random probability approach and maximising participation

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

- each organisation loaded in the main survey sample was called either a minimum of 7 times or until an interview was achieved, a refusal was given, or information was obtained to make a judgment on the eligibility of that contact
- each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. Evening and weekend interviews were also offered if the respondent preferred these times

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

- interviewers could send the reassurance email to prospective respondents if the respondent requested this
- Ipsos MORI set up an email inbox and free (0800) phone number for respondents to be able to contact to set up appointments or, in the case of the phone number, take part there and then in interviews. Where we had email addresses on the sample for organisations, we also sent four warm-up and reminder emails across the course of fieldwork to let businesses know that an Ipsos MORI interviewer would attempt to call them. These were generic email addresses, rather than ones for specific individuals in the business
- the survey had its own web page [on GOV.UK](#) to let businesses know that the contact from Ipsos MORI was genuine. The web pages included appropriate Privacy Notices on the processing of personal data, and the data rights of participants, following the introduction of GDPR in May 2018
- the survey was endorsed by the National Cyber Security Centre (NCSC), the Home Office, the Scottish Government, Confederation of British Industry (CBI), the Institute of Chartered Accountants in England and Wales (ICAEW), and the Charity Commission for England and Wales, meaning that they allowed their identity and logos to be used in the survey introduction and on the microsite to encourage businesses to take part
- as an extra encouragement, we offered to email respondents a copy of the report once published, following their interview
- specifically, to encourage participation from very large businesses, Ipsos MORI offered a £10 charity donation as a thank you for their time

Fieldwork monitoring

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

Online follow-up survey to revalidate cost data – Pilot phase only

During the pilot stage 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 questions regarding the cost of incidents in the survey and change them if they wished.

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).

We decided not to go ahead with using this during the main stage due to the relatively low uptake and results showing that the answers provided during the call matched up to those in the online survey in nearly all cases.

2.5 Fieldwork outcomes and response rate

We monitored fieldwork outcomes and response rates throughout fieldwork, and interviewers were given regular guidance on how to avoid common reasons for refusal. Table 2.3 shows the final outcomes and the adjusted response rate calculations for businesses and charities.⁵

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

Outcome	Businesses	Charities
Total sample loaded	7,848	1,405
Completed interviews	1,205	536
Incomplete interviews	330	60
Ineligible leads – established during screener ⁶	556	34
Refusals ⁷	5671	852

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

The adjusted response rates for businesses (15%) and charities (38%) are similar to the overall response rates observed in CSBS 2021 (19% for businesses and 32% for charities). The difference in response rates for businesses is likely to be due to the different sample profiles in the two surveys, as CSBS surveys a representative sample of (all) businesses while the Cyber Security Longitudinal Survey focuses on medium and large businesses that empirically have lower response rates. Additionally, response rates among businesses continue to be impacted by a combination of ongoing COVID-19 restrictions and the ongoing challenge of declining response rates in survey fieldwork in general. The increase in the response rate for charities may, in part, have been due to having the option of online completion which helped to boost the overall response rate among this audience.

The COVID-19 restrictions and the overall environment under which fieldwork took place meant:

- it was harder to reach organisations via landline numbers as many switchboards were no longer running or had a skeleton service
- when we did get through, it was harder to reach the right individual within the organisation. This is because they may have been working remotely rather than in an office or placed on furlough

⁵ The adjusted response rate with estimated eligibility is calculated as: Completed interviews / (Completed interviews + Incomplete interviews + Refusals expected to be eligible if screened + Any working numbers expected to be eligible). This calculation adjusts for the ineligible proportion of the total sample used.

⁶ Ineligible leads include sole traders, public sector organisations or the small number of organisations that self-identify as having no computer, website or online interaction.

⁷ This measure of Refusals excludes “soft” refusals. Where a respondent is initially hesitant about taking part but does not refuse outright, the interviewer will usually code as a soft refusal and call back at an alternative time.

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

- where we did reach the right person, these individuals were often busier than in previous years due to the overall strain that the pandemic placed on IT and cyber teams. As such, they were 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.

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 restrictions, then we must consider whether the businesses most negatively impacted by COVID-19 are likely to have different cyber security challenges or require different approaches to the issue – we have no strong reasons to believe this.

2.6 Data processing and weighting

Editing and data validation

There were logic checks, both in the CATI and online scripts, which checked the consistency and likely accuracy of answers estimating costs and time spent dealing with incidents. 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.

Coding

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 charity sample is unweighted. Since they were sampled through a simple random sample approach, there were no sample skews to be corrected through weighting.

For the business sample 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.

Rim weighting is an appropriate statistical technique to use for market research data with a small number of demographic variables.

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>).

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

Rim weighting allows a greater number of weighting totals to be used, since there is no longer a requirement to have all the weighting totals in one single table. It also results in less variable weights. An algorithm is used to weight the data. Technically put, rim weighting uses an iterative proportional fitting procedure. This means the sample is weighted to a series of weighting totals in turn. For example, we are weighting businesses to size and industrial sector. At the first step a starting weight is created that makes the size distribution of the sample match that of the population. This starting weight is then adjusted in all further iterations. The sample is in turn weighted to sector. At each step the weight is refined until the weighted sample matches all weighting totals within an acceptable margin of error.

We did not weight by region because region was not considered to be relevant to the survey's aim. Moreover, the final weighted data are already closely aligned with the business population region profile. The population profile data came from the BEIS Business Population Estimates 2020.

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

Table 2.4 shows the unweighted and weighted profiles of the final data. The percentages are rounded so do not always add to 100 per cent.

Table 2.4: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Medium (50–249 staff)	69%	82%
Large (250-499 staff)	14%	9%
Very large (500+)	16%	9%
Sector		
Utilities or production	1%	1%
Manufacturing	17%	16%
Construction	6%	5%
Retail or wholesale (including vehicle sales and repairs)	14%	14%
Transport or storage	5%	5%
Food or hospitality	9%	10%
Information or communication	6%	9%
Finance or insurance	3%	4%
Real estate	2%	1%
Professional, scientific or technical	10%	8%
Administration	12%	12%
Education (excluding public sector schools, colleges and universities)	2%	3%
Health, social care or social work (excluding NHS)	10%	9%
Arts or recreation	3%	2%
Service or membership organisations	1%	1%

2.7 SPSS data uploaded to UK Data Archive

Derived variables

For the questions in the survey estimating the financial costs of incidents, respondents were asked to give either an approximate numeric response or, if they did not know, then a banded response.

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 the approach taken in the Cyber Security Breaches Survey. This ensures that no survey data goes unused and 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)

Due to the costs of the most disruptive incident in the last year being collected in four constituent questions, and the overall financial cost of all incidents in the last year being collected in one subsequent separate question, direct comparisons between the two data sources should be avoided.

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 is because there is negative correlation between cost and frequency, meaning the mean of each band will skew slightly towards the lower end. Therefore, imputing values based on mid-points would slightly overestimate the true values across respondents.

Derived combined cost variable

A new derived combined cost variable was also added, summing the answers given to individual granular cost questions on short-term (damagedirs) and long-term (damagedirl) direct costs, staff time costs (damagestaff) and other indirect costs (damageind) incurred due to the most disruptive incident in the last twelve months.

This was provided as a derived variable, in addition to the data from the separate question asking for the overall cost of all incidents experienced in the last twelve months. As stated above direct comparisons should be avoided, but the derived variable can be considered an alternative approach to capturing the associated costs of incidents to organisations.

To run the calculations for the derived variable, DCMS and Ipsos MORI agreed on the following rules:

- Where respondents did not reply to all four questions, partial data was included in the calculation. For example, if a respondent answered don't know or refused to answer any of the four questions used in the calculation, their other answer(s) were still included in the total.
- Don't know and refused answer codes were coded as missing and were not used in the calculations.
- Where the response was zero, this was counted as zero.

The survey also asked the total estimated costs organisations incurred from all the identified incidents over the last twelve months (q_cost). When comparing the two, the mean and median costs are bigger (in most cases) for the derived combined cost variable than for the overall cost question asked in the survey.

Results from this analysis can be found in Table 2.5 below.

Table 2.5: Derived combined cost of most disruptive incident vs. overall cost of all incidents identified in the last year

	All businesses		Medium businesses		Large businesses		All charities	
	Derived combined	Overall cost	Derived combined	Overall cost	Derived combined	Overall cost	Derived combined	Overall cost
	Across organisations identifying any incidents							
Mean cost	£3260	£2920	£2780	£2160	£4920	£6500	£1524	£1878
Median cost	£10	£0	£5	£0	£26	£34	£10	£0
Base	800	770	557	538	243	232	375	365
	Only across organisations identifying incidents with an outcome							
Mean cost	£10567	£8410	£9423	£5530	£14066	£17010	£2881	£4420
Median cost	£500	£1000	£453	£600	£708	£2280	£600	£1425
Base	201	195	120	116	81	79	81	76

This discrepancy between the mean and median figures may be the result of:

- Respondents not being forced to give consistent answers in the survey script due to the complexities around doing that.
- Respondents may not consider all four granular cost elements when answering the overall cost question in the survey (or consider there to be some overlaps).

Redaction of cost data

No numeric £ variables were 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 were 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 incidents:

- the estimated direct short-term cost of the most disruptive incident (damagedirsx_bands)
- the estimated direct long-term cost (damagedirix_bands)
- the estimated staffing cost (damagestaffx_bands)
- the estimated damage or disruption cost (damagelindx_bands)
- the estimated cost of all incidents identified in the last 12 months (cost_bands)

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

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.⁹ 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.

⁹ The default SPSS setting is to round cell counts and then calculate percentages based on integers.

Chapter 3: Qualitative approach technical details

The qualitative strand of this research also focused on medium and large businesses and high-income charities.

3.1 Sampling

We took the sample for the 30 in-depth interviews from the quantitative survey. We asked respondents during the survey whether they would be willing to be recontacted specifically to take part in a further 45-minute interview on the same topic. In total, 1,204 respondents (69%), including 822 businesses (68%) and 382 charities (71%), agreed to be recontacted.

We carried out interviews with 18 businesses and 12 charities.

3.2 Recruitment quotas and screening

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

We used recruitment quotas to ensure that interviews included a mix of different sizes, sectors, and regions for businesses as well as different charitable areas, income bands, and countries for charities.

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.

Fieldwork

The Ipsos MORI research team carried out all fieldwork in July and August 2021. We conducted the 30 interviews through a mix of telephone and Microsoft Teams calls. Interviews lasted around 45-60 minutes on average.

DCMS originally laid out their topics of interest for these interviews. Ipsos MORI then drafted the interview topic guide around these topics, which was reviewed and approved by DCMS. The guide covered the following broad questions:

- How do organisations govern cyber? What kind of governance processes do they have in place?
- What technical controls / processes do organisations have in place? What informs these / what motivated organisations to introduce these?
- How do organisations decide their cyber risk management and level of investment in cyber security? What information informs this decision?
- Do organisations keep cyber incident records? If so, what do they record? Does this information get reported to the board? If so, how? Are they reported to anybody else or discussed at committees?
- What designated roles and responsibilities do organisations have in place related to cyber?
- How do organisations manage supplier risks from their immediate suppliers? How do organisations manage risk in the wider supply chain?
- How do organisations use external cyber/IT consultants?

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

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

Tables 3.1 and 3.2 show a profile of the 18 interviewed businesses by size and sector.

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

SIC 2007 letter	Sector description	Total
B, C, D, E	Utilities or production (including manufacturing)	3
F	Construction	2
G	Retail or wholesale (including vehicle sales and repairs)	2
H	Transport or storage	1
I	Food or hospitality	0
J	Information or communications	1
K	Finance or insurance	3
L, N	Administration or real estate	2
M	Professional, scientific or technical	3
P	Education (excluding state education institutions)	0
Q	Health, social care or social work	0
R, S	Entertainment, service or membership organisations	1
	Total	18

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

Size band	Total
Medium (50-249 staff)	7
Large (250-499 staff)	5
Very large (500+ staff)	6

3.3 Analysis

Throughout fieldwork, the core research team discussed interim findings. We held two analysis meetings over Ms Teams 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.

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 listened back to recordings in order to identify 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. The burden imposed should also 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.¹⁰

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 **1,741 respondents** and the average (mean) survey length was **22 minutes**. Therefore, the research compliance cost for the quantitative survey this year was [1,741 × 22 minutes = **638 hours**]
- the qualitative research had **30 respondents** and the average interview length was **50 minutes**. Respondents completed the qualitative interviews in addition to the quantitative survey. The research compliance cost for the qualitative strand this year was [30 × 50 minutes = **25 hours**]

In total, the compliance cost for the Cyber Longitudinal Survey Wave 1 was **663 hours**.

Steps taken to minimise the research burden

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

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

¹⁰ The report authors consulted with professional GSS Government Social Research (GSR) guidelines: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1000708/2021-GSR_Ethics_Guidance_v3.pdf

Appendix A: Questionnaire

Consent

Q_CONSENT

ASK IF CATI

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?

SINGLE CODE

1. Yes
2. No [CLOSE SURVEY]

Screener

Q_TYPE

ASK IF IDBR SAMPLE (S_SAMPLETYPE=_01)

Is your organisation a registered charity in the UK?

SINGLE CODE

1. Yes – registered charity
2. No – not a registered charity

Q_TYPEDUM

DUMMY VARIABLE NOT ASKED

SINGLE CODE

1. IF TYPE CODE 2: Business
2. IF TYPE CODE 1 OR S_SAMPLETYPE=_02: Charity

SCRIPT TO BASE [BUSINESS/CHARITY] TEXT SUBSTITUTIONS ON TYPEDUM (CHARITY IF TYPEDUM CODE 2, ELSE BUSINESS)

Q_SIZEA

ASK IF BUSINESS (TYPEDUM CODE 1)

Including yourself, how many staff work for your organisation across the UK as a whole?

CATI: ADD IF NECESSARY: We mean both full-time and part-time employees on your payroll, as well as any directors, working proprietors or owners.

WRITE IN RANGE 50–500,000 (SOFT CHECK IF >9,999)

SINGLE CODE

1. CATI: DO NOT READ OUT: Under 50 [CLOSE SURVEY]
2. CATI: DO NOT READ OUT: Don't know

Q_SIZEB

ASK IF DON'T KNOW SIZE OF ORGANISATION (SIZEA CODE DK)

Which of the following best represents the number of staff working for your organisation across the UK as a whole, including yourself?

CATI: PROBE FULLY

SINGLE CODE

1. Under 50 [CLOSE SURVEY]
2. 50 to 249
3. 250 to 499
4. 500 to 999
5. 1,000 or more
6. CATI: DO NOT READ OUT: Don't know [CLOSE SURVEY]

Q_SIZEDUM

DUMMY VARIABLE NOT ASKED

MERGE RESPONSES FROM SIZEA AND SIZEB

SINGLE CODE

1. 50 to 249
2. 250 to 499
3. 500 to 999
4. 1,000 or more

Q_INCOME

ASK IF IDBR SAMPLE AND CHARITY (TYPE CODE 1)

In the last financial year, was the annual income of your charity £1 million or higher?

SINGLE CODE

1. Yes – £1 million or higher
2. No – under £1 million [CLOSE SURVEY]

Digital infrastructure within the organisation

Q_ONLINE

ASK ALL

ASK AS A GRID

RANDOMISE LIST BUT KEEP A/B TOGETHER

Does your organisation currently use or provide any of the following?

CATI: READ OUT

- a) A cloud server that stores your data or files
- b) Your own physical server that stores your data or files
- c) A virtual private network, or VPN, for staff connecting remotely

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_DEVICES

ASK ALL

Are staff permitted to access your organisation's network or files through personally owned devices (e.g. a personal smartphone or home computer)?

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_VPN

ASK IF HAVE VPN (ONLINEc CODE 1)

If staff connect to your network or files **outside** your own workplaces, are they forced to connect via a VPN, or can they access your network or files without a VPN?

CATI: PROBE FULLY

CATI: ADD IF NECESSARY: By VPN, we mean a Virtual Private Network.

SINGLE CODE

1. Forced to connect via a VPN
2. Can connect without a VPN
3. CATI: DO NOT READ OUT: Not applicable/ No remote working
4. CATI: DO NOT READ OUT: Don't know

Policies and processes

PROCESS

READ OUT IF CATI ONLY

Now I would like to ask some questions about your 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.

Q_IDENT

ASK ALL

ASK AS A GRID

RANDOMISE LIST

Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation?

CATI: READ OUT

- a) A cyber security vulnerability audit
- b) A risk assessment covering cyber security risks
- c) Invested in threat intelligence
- d) Used specific tools designed for security monitoring, such as Intrusion Detection Systems

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_AIML

ASK ALL

Does your organisation deploy any cyber security tools that use AI or machine learning?

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_RULES

ASK ALL

ASK AS A GRID

RANDOMISE LIST BUT KEEP D AND E TOGETHER

And which of the following rules or controls, if any, do you have in place?

CATI: READ OUT

- a) A policy to apply software security updates within 14 days
- b) Any monitoring of user activity
- c) Specific rules for storing and moving files containing people's personal data
- d) Backing up data securely via a cloud service
- e) Backing up data securely via other means
- f) Up-to-date malware protection across all your devices
- g) Firewalls that cover your entire IT network, as well as individual devices
- h) Restricting IT admin and access rights to specific users
- i) Security controls on your organisation's own devices (e.g. laptops)

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_GOV

ASK ALL

ASK AS A GRID

RANDOMISE LIST

Does your organisation have any of the following documentation in place to help manage cyber security risks?

CATI: READ OUT

- a) A Business Continuity Plan that covers cyber security
- b) A risk register that covers cyber security
- c) Any documentation that outlines how much cyber risk your organisation is willing to accept
- d) Any documentation that identifies the most critical assets that your organisation wants to protect
- e) A written list of your organisation's IT estate and vulnerabilities

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_TRAINED

ASK ALL

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

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_COMPLY**ASK ALL****RANDOMISE LIST BUT KEEP CODES 2/3 TOGETHER AND 4/5 TOGETHER**

Which of the following standards or accreditations, if any, does your organisation adhere to?

CATI: READ OUT**MULTICODE**

1. ISO 27001
2. The Cyber Essentials standard
3. The Cyber Essentials Plus standard

SINGLE CODE**NOT PART OF ROTATION**

4. **CATI: DO NOT READ OUT:** None of these
5. **CATI: DO NOT READ OUT:** Don't know

Q_STATEMENT**ASK ALL**

Did you include anything about cyber security in your organisation's most recent annual report?

SINGLE CODE

1. Yes
2. No
3. **CATI: DO NOT READ OUT:** Don't know
4. **CATI: DO NOT READ OUT:** Not applicable – do not have annual reports

Supplier risks**Q_SUPPLYRISK****ASK ALL****IF BUSINESS:** This question is about your supply chain. This is not just security or IT suppliers. It includes any immediate suppliers that provide goods or services to your organisation, and their own suppliers (i.e. your subcontractors).**IF CHARITY:** This question is about third-party organisations you work with. This includes any immediate suppliers that provide goods or services to your organisation, and their own suppliers (i.e. your subcontractors). It also includes partners such as other charities.In the last 12 months, has your organisation carried out any work to formally assess or manage the potential cyber security risks presented by any of these suppliers **[IF CHARITY: or partners]**?**SINGLE CODE**

1. Yes
2. No
3. **CATI: DO NOT READ OUT:** Don't know

Q_SUPPLYHOW**ASK IF REVIEWED IMMEDIATE SUPPLIER RISKS (SUPPLYRISK CODE 1)****ASK AS A GRID****RANDOMISE LIST**Which of the following, if any, have you done with any of your suppliers **[IF CHARITY: or**

partners] in the last 12 months?

CATI: READ OUT

- a) Carried out a formal assessment of their cyber security, e.g. an audit
- b) Set minimum cyber security standards in supplier contracts
- c) Requested cyber security information on their own supply chains
- d) Given them information or guidance on cyber security
- e) Stopped working with a supplier following a cyber incident

SINGLE CODE

- 1. Yes
- 2. No
- 3. CATI: DO NOT READ OUT: Don't know

Improvements

Q_IMPROVE

ASK ALL

ASK AS A GRID

RANDOMISE LIST

Now we want to ask about the things that may have changed in the last 12 months.

In this time, has your organisation taken any steps to **expand or improve** any of the following aspects of your cyber security?

CATI: READ OUT

- a) Your processes for updating and patching systems and software
- b) IF MONITOR USERS (RULESb CODE 1): The way you monitor your users
- c) Your processes for managing cyber security incidents
- d) Your malware defences
- e) Your processes for user authentication and access control
- f) The way you monitor systems or network traffic
- g) Your network security

SINGLE CODE

- 1. Yes
- 2. No
- 3. CATI: DO NOT READ OUT: Don't know
- 4. CATI: DO NOT READ OUT: Not applicable/do not have this

Influencers

Q_PEER

ASK ALL

ASK AS A GRID

RANDOMISE LIST

In the last 12 months, have you ever reviewed or changed any cyber security policies or processes as a result of the following?

CATI: READ OUT

- a) Another organisation in your sector experiencing a cyber security incident
- b) Another organisation in your sector implementing similar measures

SINGLE CODE

1. Yes
2. No
3. **CATI: DO NOT READ OUT:** Don't know

Q_INFLUENCE

ASK ALL

ASK AS A GRID

RANDOMISE LIST BUT KEEP A/B TOGETHER

REVERSE SCALE EXCEPT DK AND N/A

Over the last 12 months, how much have your actions on cyber security been influenced by feedback from any of the following groups?

CATI: READ OUT

- a) External IT or cyber security consultants
- b) **IF BUSINESS:** Any investors or shareholders
- c) **IF BUSINESS:** Your customers
- d) Regulators for your sector
- e) Your insurers
- f) Whoever audits your accounts

SINGLE CODE

1. A great deal
2. A fair amount
3. Not very much
4. Not at all
5. **CATI: DO NOT READ OUT:** Don't know
6. **CATI: DO NOT READ OUT:** Not applicable/do not have these

Cyber insurance

Q_INSUREX

ASK ALL

There are general insurance policies that provide cover for cyber security incidents, among other things. There are also specific insurance policies that are solely for this purpose. Which of the following best describes your situation?

CATI: READ OUT

SINGLE CODE

1. We have a specific cyber security insurance policy
2. We have cyber security cover as part of a broader insurance policy
3. We are not insured against cyber security incidents
4. **CATI: DO NOT READ OUT:** Don't know

Board engagement

BOARD

READ OUT TO ALL

The next questions ask about your management board. By this, we mean the board of directors or trustees, as well as senior leadership like a Chief Executive.

Q_BOARDGOVERN

ASK ALL

ASK AS A GRID

RANDOMISE LIST

Does your organisation have any of the following?

CATI: READ OUT

- a) One or more board members whose roles include oversight of cyber security risks
- b) A designated staff member responsible for cyber security, who reports directly to the board

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_BOARDDISCUSS

ASK ALL

REVERSE SCALE EXCEPT DK

Over the last 12 months, roughly how often, if at all, has your board discussed or received updates on your organisation's cyber security? Is it ...

CATI: PROBE FULLY

SINGLE CODE

1. Never
2. Once a year
3. Once every 6 months
4. Quarterly
5. Monthly
6. Weekly
7. Daily
8. CATI: DO NOT READ OUT: Don't know

Q_BOARDENGAGE

ASK IF BOARD DISCUSSES CYBER SECURITY (DISCUSS NOT CODE 1)

REVERSE SCALE EXCEPT DK

This question is about how your board typically engages with any information on the cyber security risks your organisation faces.

How much would you agree or disagree with the following statement?

CATI: READ OUT

- a) The board integrates cyber risk considerations into wider business areas

SINGLE CODE

1. Strongly agree
2. Tend to agree
3. Neither agree nor disagree
4. Tend to disagree

5. Strongly disagree
6. CATI: DO NOT READ OUT: Don't know

Q_BOARDTRAIN

ASK ALL

Have any of the board received any cyber security training?

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Information sources

Q_NCSC

ASK ALL

In the last 12 months, has your organisation used any information or guidance from the National Cyber Security Centre (NCSC) to inform your approach to cyber security?

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_GUIDANCE

ASK IF USED NCSC GUIDANCE (NCSC CODE 1)

RANDOMISE LIST

Which of the following, if any, have you used?

CATI: READ OUT

MULTICODE

1. NCSC weekly threat reports
2. The 10 Steps to Cyber Security
3. The Cyber Security Board Toolkit
4. NCSC guidance on secure home working or video conferencing
5. NCSC guidance for moving your business online
6. NCSC's Cyber Assessment Framework

SINGLE CODE

7. CATI: DO NOT READ OUT: None of these
8. CATI: DO NOT READ OUT: Don't know

Experience of incidents

INCIDREADOUT

READ OUT IF CATI ONLY

Now I'd like to ask some questions about cyber security incidents. In the next question, we go through a list of what we mean by cyber security incidents.

Q_INCIDENT

ASK ALL

ASK AS A GRID

RANDOMISE LIST BUT KEEP A/B, C/D AND F/G TOGETHER

Have any of the following happened to your organisation in the last 12 months?

CATI: READ OUT

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

- a) Devices becoming infected with ransomware
- b) Devices becoming infected with other malware (e.g. viruses, Trojans or spyware)
- c) Unauthorised accessing of files, devices, networks or servers by staff, even if accidental
- d) Unauthorised accessing of files, devices, networks or servers by people outside your organisation
- e) Attacks that try to slow or take down your website, applications or online services, i.e. denial of service attacks
- f) Attempted hacking of online bank accounts
- g) Attempted hacking of your website, social media or user accounts
- h) People impersonating your organisation in emails or online
- i) Staff receiving fraudulent emails or attachments, or arriving at fraudulent websites i.e. phishing attacks
- j) Unauthorised listening into video conferences or instant messaging

NOT PART OF RANDOMISATION

- k) Any other types of cyber security incidents

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know
4. CATI: DO NOT READ OUT: Prefer not to say

Q_FREQ

ASK IF ANY CYBER SECURITY INCIDENTS (ANY INCIDENT_{a-k} CODE 1)

Approximately, how often in the last 12 months did you experience any of the cyber security incidents you mentioned? Was it...?

CATI: READ OUT

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

SINGLE CODE

1. Once only
2. More than once but less than once a month
3. Roughly once a month
4. Roughly once a week
5. Roughly once a day
6. Several times a day
7. CATI: DO NOT READ OUT: Don't know
8. CATI: DO NOT READ OUT: Prefer not to say

Q_OUTCOME

ASK IF ANY CYBER SECURITY INCIDENTS (ANY INCIDENT_{a-k} CODE 1)

ASK AS A GRID

RANDOMISE LIST BUT KEEP A/B AND C/D TOGETHER

Thinking of all the cyber security incidents experienced in the last 12 months, which, if any, of the following happened as a result?

CATI: READ OUT

- a) Permanent loss of files (other than personal data)
- b) Temporary loss of access to files or networks
- c) Money was stolen
- d) Money was paid as a ransom
- e) Software or systems were corrupted or damaged
- f) Personal data (e.g. on [IF BUSINESS: customers or staff/IF CHARITY: beneficiaries, donors, volunteers or staff]) was altered, destroyed or taken
- g) Lost or stolen assets, trade secrets or intellectual property
- h) Your website, applications or online services were taken down or made slower
- i) Lost access to any third-party services you rely on
- j) Physical devices or equipment were damaged or corrupted
- k) Compromised accounts or systems used for illicit purposes (e.g. launching attacks)

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_IMPACT

ASK IF ANY CYBER SECURITY INCIDENTS (ANY INCIDENT_{a-k} CODE 1)

ASK AS A GRID

RANDOMISE LIST BUT KEEP A/B TOGETHER

And have any of these incidents impacted your organisation in any of the following ways?

CATI: READ OUT

- a) Additional staff time to deal with the incident, or to inform [IF BUSINESS: customers/IF CHARITY: beneficiaries] or stakeholders
- b) Any other repair or recovery costs
- c) Stopped staff from carrying out their day-to-day work
- d) Loss of [IF BUSINESS: revenue or share value/IF CHARITY: income]
- e) New measures needed to prevent or protect against future incidents
- f) Fines from regulators or authorities, or associated legal costs
- g) Reputational damage
- h) Prevented provision of goods or services to [IF BUSINESS: customers/IF CHARITY: beneficiaries or service users]
- i) Discouraged you from carrying out a future business activity you were intending to do
- j) Complaints from [IF BUSINESS: customers/IF CHARITY: beneficiaries or stakeholders]
- k) Goodwill compensation or discounts given to customers

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_RANSOM

ASK ALL

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

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Most disruptive incident

ONEINCIDENTA

READ OUT IF CATI/SHOWSCREEN IF WEB AND MORE THAN ONE TYPE OF INCIDENT EXPERIENCED (2 OR MORE INCIDENTa-k CODE 1)

Now we would like you to think about the one cyber security incident, or related series of incidents, that caused the most disruption to your organisation in the last 12 months.

Q_DISRUPT

ASK IF MORE THAN ONE TYPE OF INCIDENT EXPERIENCED (2 OR MORE INCIDENTa-k CODE 1)

CODES ARE THE STATEMENTS WHERE CODE 1 AT INCIDENT

What kind of incident was this?

CATI: PROMPT TO CODE IF NECESSARY

CATI: INTERVIEWER NOTE: IF MORE THAN ONE CODE APPLIES, ASK RESPONDENT WHICH ONE OF THESE THEY THINK STARTED OFF THE INCIDENT

SINGLE CODE

1. CATI: DO NOT READ OUT: Don't know

ONEINCIDENTB

READ OUT IF CATI/SHOWSCREEN IF WEB AND EXPERIENCED ONE TYPE OF INCIDENT MORE THAN ONCE ([ONLY 1 INCIDENTa-k CODE 1] AND [FREQ CODES 2-6 OR DK])

You mentioned you had experienced [INSERT STATEMENT WHERE CODE 1 AT INCIDENT] on more than one occasion. Now we would like you to think about the one instance of this that caused the most disruption to your organisation in the last 12 months.

Q_RESTORE

ASK IF ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTa-k CODE 1] OR DISRUPT CODES A-K)

How long, if any time at all, did it take to restore business operations back to normal after the incident was identified? Was it...?

CATI: PROBE FULLY

SINGLE CODE

1. No time at all
2. Less than a day
3. Between a day and under a week
4. Between a week and under a month
5. One month or more
6. CATI: DO NOT READ OUT: Still not back to normal
7. CATI: DO NOT READ OUT: Don't know

Incident costs

EXPLORECOSTSCATI

READ OUT IF CATI AND ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTA-K CODE 1] OR DISRUPT NOT DK)

I am now going to ask you about the approximate costs of this particular incident.

EXPLORECOSTSWEB

SHOWSCREEN IF WEB AND ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTA-K CODE 1] OR DISRUPT NOT DK)

The next questions are about the approximate costs of this particular incident. As a reminder, all the questions in this survey are confidential.

Q_DAMAGEDIRS

ASK IF ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTA-K CODE 1] OR DISRUPT NOT DK)

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.

CATI: PROBE FOR BEST ESTIMATE BEFORE CODING DK

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£9,999,999

SOFT CHECK IF >£9,999

SINGLE CODE

1. CATI: DO NOT READ OUT: No cost of this kind incurred
2. CATI: DO NOT READ OUT: Don't know
3. CATI: DO NOT READ OUT: Prefer not to say

Q_DAMAGEDIRSB

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY INCIDENT (DAMAGEDIRS CODE DK)

Was it approximately...?

CATI: PROMPT TO CODE

SINGLE CODE

1. Less than £100
2. £100 to less than £500
3. £500 to less than £1,000
4. £1,000 to less than £5,000
5. £5,000 to less than £10,000
6. £10,000 to less than £20,000
7. £20,000 to less than £50,000
8. £50,000 to less than £100,000
9. £100,000 to less than £500,000
10. £500,000 to less than £1 million

11. £1 million to less than £5 million
12. £5 million or more
13. CATI: DO NOT READ OUT: Don't know

Q_DAMAGEDIRL

ASK IF ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTA-K CODE 1] OR DISRUPT NOT DK)

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.

CATI: PROBE FOR BEST ESTIMATE BEFORE CODING DK

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£9,999,999

SOFT CHECK IF >£9,999

SINGLE CODE

1. CATI: DO NOT READ OUT: No cost of this kind incurred
2. CATI: DO NOT READ OUT: Don't know
3. CATI: DO NOT READ OUT: Prefer not to say

Q_DAMAGEDIRLB

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY INCIDENT (DAMAGEDIRL CODE DK)

Was it approximately...?

CATI: PROMPT TO CODE

SINGLE CODE

1. Less than £100
2. £100 to less than £500
3. £500 to less than £1,000
4. £1,000 to less than £5,000
5. £5,000 to less than £10,000
6. £10,000 to less than £20,000
7. £20,000 to less than £50,000
8. £50,000 to less than £100,000
9. £100,000 to less than £500,000
10. £500,000 to less than £1 million
11. £1 million to less than £5 million
12. £5 million or more
13. CATI: DO NOT READ OUT: Don't know

Q_DAMAGESTAFF

ASK IF ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTA-K CODE 1] OR DISRUPT NOT DK)

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.

CATI: PROBE FOR BEST ESTIMATE BEFORE CODING DK

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£9,999,999

SOFT CHECK IF >£9,999

SINGLE CODE

1. CATI: DO NOT READ OUT: No cost of this kind incurred
2. CATI: DO NOT READ OUT: Don't know
3. CATI: DO NOT READ OUT: Prefer not to say

Q_DAMAGESTAFFB

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY INCIDENT (Q_DAMAGESTAFF CODE DK)

Was it approximately...?

CATI: PROMPT TO CODE

SINGLE CODE

1. Less than £100
2. £100 to less than £500
3. £500 to less than £1,000
4. £1,000 to less than £5,000
5. £5,000 to less than £10,000
6. £10,000 to less than £20,000
7. £20,000 to less than £50,000
8. £50,000 to less than £100,000
9. £100,000 to less than £500,000
10. £500,000 to less than £1 million
11. £1 million to less than £5 million
12. £5 million or more
13. CATI: DO NOT READ OUT: Don't know

Q_DAMAGEIND

ASK IF ONLY ONE TYPE OF INCIDENT EXPERIENCED OR IF CAN CONSIDER A PARTICULAR INCIDENT ([ONLY 1 INCIDENTA-K CODE 1] OR DISRUPT NOT DK)

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.

CATI: PROBE FOR BEST ESTIMATE BEFORE CODING DK

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£9,999,999|

SOFT CHECK IF >£9,999

SINGLE CODE

- 1. CATI: DO NOT READ OUT: No cost of this kind incurred
- 2. CATI: DO NOT READ OUT: Don't know
- 3. CATI: DO NOT READ OUT: Prefer not to say

Q_DAMAGEINDB

ASK IF DON'T KNOW DIRECT RESULT COST OF THIS CYBER SECURITY INCIDENT
(Q_DAMAGEIND CODE DK)

Was it approximately...?

CATI: PROMPT TO CODE

SINGLE CODE

- 1. Less than £100
- 2. £100 to less than £500
- 3. £500 to less than £1,000
- 4. £1,000 to less than £5,000
- 5. £5,000 to less than £10,000
- 6. £10,000 to less than £20,000
- 7. £20,000 to less than £50,000
- 8. £50,000 to less than £100,000
- 9. £100,000 to less than £500,000
- 10. £500,000 to less than £1 million
- 11. £1 million to less than £5 million
- 12. £5 million or more
- 13. CATI: DO NOT READ OUT: Don't know

Q_COSTA

ASK IF ANY CYBER SECURITY INCIDENTS (ANY INCIDENTA-K CODE 1)

Considering all these different costs, how much do you think **all** the cyber security incidents you have experienced in the last 12 months have cost your organisation financially?

CATI: PROBE FOR BEST ESTIMATE BEFORE CODING DK

CATI: REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF

WRITE IN RANGE £1–£30,000,000

IF MEDIUM (SIZEA 49<CODE<250 OR SIZEDUM CODE 1): SOFT CHECK IF <£100 OR >£99,999

IF LARGE (SIZEA 249<CODE OR [SIZEDUM CODES 2–4]): SOFT CHECK IF <£1,000 OR >£99,999

SINGLE CODE

- 1. CATI: DO NOT READ OUT: No cost incurred
- 2. CATI: DO NOT READ OUT: Don't know
- 3. CATI: DO NOT READ OUT: Prefer not to say

Q_COSTB

ASK IF DON'T KNOW TOTAL COST OF CYBER SECURITY INCIDENTS (COSTA CODE DK)

Was it approximately...?

CATI: PROMPT TO CODE

SINGLE CODE

1. Less than £100
2. £100 to less than £500
3. £500 to less than £1,000
4. £1,000 to less than £5,000
5. £5,000 to less than £10,000
6. £10,000 to less than £20,000
7. £20,000 to less than £50,000
8. £50,000 to less than £100,000
9. £100,000 to less than £500,000
10. £500,000 to less than £1 million
11. £1 million to less than £5 million
12. £5 million or more
13. CATI: DO NOT READ OUT: Don't know

Cyber security incident management

Q_INCIDMAN

ASK ALL

Do you have any written processes for how to manage a cyber security incident, for example, an incident response plan?

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_INCIDCONTENT

ASK IF HAVE INCIDENT MANAGEMENT PROCESSES (INCIDMAN CODE 1)

ASK AS A GRID

RANDOMISE LIST

And which of these, if any, is covered in your written incident management processes?

CATI: READ OUT

- a) Guidance for reporting incidents externally, e.g. to regulators or insurers
- b) Any legal or regulatory requirements
- c) Communications and public engagement plans

SINGLE CODE

1. Yes
2. No
3. CATI: DO NOT READ OUT: Don't know

Q_EXERCISE

ASK IF HAVE INCIDENT MANAGEMENT PROCESSES (INCIDMAN CODE 1)

In the last 12 months, have you carried out any cyber incident exercises to test your incident response policies and processes?

CATI: READ OUT

SINGLE CODE

1. Yes
2. No

3. **CATI: DO NOT READ OUT:** Don't know

ASK IF CATI AND PART OF INCENTIVE GROUP (S_INCENTIVE=_01)

As promised, we will make a £10 charity donation on your behalf as a thank you for taking part. We have three charities for you to choose from:

- The NHS Charities Together COVID-19 Appeal
- The NSPCC
- Samaritans

ADD IF NECESSARY:

- The NHS Charities Together COVID-19 Appeal brings together over 250 charitable organisations that support the NHS in England, Scotland and Wales.
- The NSPCC, or National Society for the Prevention of Cruelty to Children, is a charity campaigning and working in child protection in the United Kingdom.
- Samaritans provides emotional support to anyone in emotional distress, struggling to cope, or at risk of suicide throughout the United Kingdom and Ireland.

SINGLE CODE

1. NHS Charities Together
2. NSPCC
3. Samaritans
4. Prefer not to donate

ADMIN

READ OUT IF CATI

Now just some administrative questions before we finish.

Q_PANELRECON

ASK ALL

DCMS expects to carry out similar research next year. Your input is really important to help the Government to better understand and respond to your organisation's cyber security needs. Would you be happy for Ipsos MORI to contact you on behalf of DCMS for your views on this topic again before the end of 2022?

[**ADD IF WEB:** You would have the opportunity to take the survey online again.]

SINGLE CODE

1. Yes
2. No

Q_QUALRECON

ASK ALL

We also want to have a more in-depth conversation on these topics with a handful of organisations. We would pay participants £50 for their time. Would you be happy to receive an invite for one of these conversations in summer 2021, if you're selected to take part?

SINGLE CODE

1. Yes
2. No

Q_NAME

ASK IF WANT RECONTACT (PANELRECON CODE 1 OR QUALRECON CODE 1)

Can we please have your name and job title for this?

CATI: INTERVIEWER NOTE: TAKE DOWN NAME, SURNAME AND JOB TITLE WITHOUT PREFIXES (MR, MRS ETC.)

WRITE IN

1. CATI: DO NOT READ OUT: Prefer not to say

Q_PUBLISHED

ASK ALL

Finally, would you like us to email you a copy of the report when it is published later this year?

SINGLE CODE

1. Yes
2. No

Q_EMAIL

ASK IF RECONTACT OR REPORT (PANELRECON CODE 1 OR QUALRECON CODE 1 OR PUBLISHED CODE 1)

Can we please take the best email address for you?

WRITE IN EMAIL IN VALIDATED FORMAT

2. CATI: DO NOT READ OUT: Prefer not to say

SCRIPT TO SEND WEB INVITE IF VALIDATE CODE 1**Q_DATA LINK**

ASK IF ANY CYBER SECURITY INCIDENTS (ANY INCIDENTA-K CODE 1)

Would it be possible for DCMS to link your responses to data sources held by the Information Commissioner's Office (ICO)?

ICO records hold information on cyber security incidents organisations reported to them.

By linking this data, we can reduce the burden of our surveys on your business and can improve the evidence that we use. We learn a lot about your experiences of incidents from the questions we ask in the study, but adding extra information from ICO records helps us to build a more complete picture of the impact of these incidents.

Consent will remain indefinite but if you wish to withdraw consent at any point, you can contact the research team at Ipsos MORI. Any data linked up to that point will remain but no future linking will take place. Data will only be used to inform DCMS operations - we will never release information that identifies any individual organisation publicly - and your survey responses remain strictly confidential.

Do you give your consent for us to do this?

SINGLE CODE

1. Yes
2. No

ENDSCREEN

READ OUT IF CATI/SHOWSCREEN IF WEB

Thank you for taking the time to participate in this study. You can access the privacy notice

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

online at: [ADD LINK](#). 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: Topic guide

Prompts and probes	Timings and notes
<p>Introduction</p> <ul style="list-style-type: none"> ● Introduce yourself and Ipsos MORI – independent research organisation (i.e., independent of government) ● Commissioned by the Department for Digital, Culture, Media & Sport (DCMS) ● Thank participant for taking part in the survey. ● Explain the research: we are speaking with organisations to explore the answers given in the survey in greater detail and learn more about how they approach cyber security and to discuss topics from the survey in more detail ● Confidentiality: all responses are confidential ● Length: around 45 minutes ● As a thank you for your time, we are offering a £50 incentive, this should be arranged by my colleague who booked in the interview with you. ● Get permission to digitally record to help with notes and for anonymised quotes for the report <p>GDPR consent (once recorder is on):</p> <ul style="list-style-type: none"> ● Ipsos MORI’s legal basis for processing is your consent to take part in this research. ● Your participation in this research is voluntary. ● You can withdraw consent for data to be used at any point during or after the interview. Can I check you are happy to proceed? 	<p>2-3 minutes</p> <p><i>The welcome helps to orientate the participant and gets them prepared to take part in the interview.</i></p> <p><i>Outlines the “rules” of the interview (including those we are required to tell them about under MRS guidelines). This includes GDPR-related consent.</i></p> <p><i>Make this very brief – we have already spoken to these individuals in the quantitative survey, so they should understand the background.</i></p>
<p>Context</p> <p>Before we begin, could you briefly describe your day-to day role and the organisation you currently work for?</p> <p>In a few words for now, how do you think the topic of cyber security affects your organisation? What would you say are the top two or three risks an organisation like yours faces?</p>	<p>2-3 minutes</p> <p><i>This section provides context to follow up on later in the interview, in terms of who is in charge and what they see as the risks.</i></p> <p><i>Make this very brief.</i></p>
<p>1. Cyber security resilience</p>	<p>12 mins</p>
<p>Thank you very much for your answers so far, the first section of our interview will focus on cyber resilience.</p> <p>Do you feel that your organisation has appropriate controls and processes in place to mitigate against cyber</p>	<p><i>This section explores the processes an organisation has in place to mitigate against, and recover from, cyber security incidents – whether they face</i></p>

incidents? PROBE TO UNDERSTAND IN DETAIL THEN FOLLOW UP: And how do you feel about the organisation's controls and processes to help recovery from cyber incidents?

- Probe to understand why yes/no
- IF YES: **What do you think are the main challenges faced by your organisation when it comes to maintaining these?**

Does your organisation have any cyber security measures in place to manage risk?

- PROBE ON: types of measures mentioned in the survey (refer to survey answers QIDENT)
- Why did you introduce these measures? IF NOT MENTIONED: Do you feel that having these cyber security measures in place gives you a competitive advantage to others in the industry?
- How effective have each of these measures been?
- Do you have cyber champions within your organisation? If so, what's their role/ what level of seniority/ which team (e.g. IT/ Compliance/ specific cyber team)? (note this for later)
- IF NO MEASURES: Probe to understand why

What kind of information, if any, does your organisation use to inform its cyber risk management strategy?

- Probe on internal types of information:
 - Internal cyber incident reports
 - Results from pen-tests
 - A risk assessment covering cyber security risks
 - Internal tools designed for security monitoring, such as Intrusion Detection Systems
 - Results from a cyber security vulnerability audit
- Probe on external types of information:
 - External sources of threat intelligence (e.g. NCSC – National Cyber Security Centre)
 - Government guidance
 - Cyber risk management standards and frameworks and associated guidance (IF NEEDED: e.g. CAF – Cyber Assessment Framework, CE – Cyber Essentials, ISO 27001 – International Information Security Standard, NIST – National Institute of Standards & Technology)
- How useful did you find this information?
 - IF USEFUL: What did you find particularly helpful?

any challenges in doing so and whether they think their level of investment is appropriate.

- IF NOT USEFUL: What could have been improved to make that information more helpful to you?

How appropriate, if at all, do you think your organisation’s investments into cyber risks management are?

Probe to understand why yes/no:

- How do you determine whether your investments into cyber risk management are appropriate?
- How have you assessed your organisation’s cyber resilience? PROBE FULLY
- IF NOT/NOT VERY APPROPRIATE:
 - What risks, if any, do you associate with that?
 - What would inform more appropriate investment in cyber risk management?

What kind of governance processes, if any, do you have in place to manage cyber security incidents?

(Explicitly explore whether they are proactive or reactive in their response to cyber threats)

- **Do you have an incident response plan?**
- IF YES:
 - What are the processes you would follow?
 - How often is the plan tested?
 - (If they have cyber champions) Are the cyber champions involved – how?
- IF NO:
 - What are your first steps after realising you’ve experienced/are experiencing a cyber security incident?
 - Do you have any general practices/steps you tend to follow?
 - Who do you inform?
 - (If they have cyber champions) Are the cyber champions involved – how?

Have you completed a cyber skills assessment of your workforce?

- IF YES: What did this involve?
- IF NO: Why?

To what extent is cyber security aligned to your organisation’s strategic priorities? Why is this?

2. Ransomware

3-4 mins

<p>Before we move on, I'd like to spend a couple of minutes talking about a specific threat. Please could you let me know if you are aware of ransomware?</p> <ul style="list-style-type: none"> IF AWARE: What do you know about it? What impact, if any, might ransomware have on your organisation? <p>Have you taken any specific actions in relation to ransomware? PROBE FULLY.</p> <ul style="list-style-type: none"> IF YES: What motivated you to take action? How would you assess the threat of ransomware compared to other risks and threats? IF NO: Are there any particular reasons why you haven't taken action? 	<p><i>This section explores the impact of ransomware on organisations, and whether they mitigate against it,</i></p> <p><i>For info: ransomware is a type of malware (malicious software) that prevents you from accessing your computer (or the data that is stored on it).</i></p>
<p>3. Record keeping & internal reporting</p>	<p>7-8 mins</p>
<p>In the next few minutes, I would like to move on to talk about the way your organisation may keep record of cyber security incidents.</p> <p>ASK ALL</p> <p>How does your organisation keep records of cyber security incidents? (note yes/no for later)</p> <p>ASK ALL WHO KEEP RECORDS</p> <ul style="list-style-type: none"> Who maintains them? What are the reasons for recording them? What information do you include in the records? How are the records used? (If they have cyber security insurance Q_INSUREX) Do you share these records with your insurer? <p>ASK ALL WHO DO NOT KEEP RECORDS</p> <ul style="list-style-type: none"> What are the reasons for not recording cyber security incidents? Probe if needed on: need, time, experience/resource Is there anything that would incentivise you to start keeping records? <p>ASK ALL</p> <p>What types of internal reports, if any, does your board receive on cyber security?</p> <p>ASK ALL WHO REPORT INTERNALLY TO BOARD</p> <ul style="list-style-type: none"> What information do they receive – why? How often is this reported to the board – why? (If they keep records of cyber security incidents) IF NOT MENTIONED: How often, if at all, do you report your cyber incident records to the board? How is this information reported to the board? 	<p><i>This section explores whether organisations keep records of their cyber security incidents and the reasons for (not) doing so.</i></p> <p><i>It also explores the role of the board and committees in their cyber security management.</i></p>

<p>ASK ALL WHO DON'T REPORT INTERNALLY TO BOARD</p> <ul style="list-style-type: none"> • What are the reasons for not reporting information related to cyber security to the board? <ul style="list-style-type: none"> - PROBE ON: need, time, experience/resource, lack of interest / lack of expertise/ understanding among board members here • What would need to change for you to report cyber security issues to the board? Is there anything that could encourage you? <p>At what committee(s), if any, is cyber security discussed?</p> <p><i>Participants may reference audit, cyber or none.</i></p> <p>ASK ALL WHO HAVE A COMMITTEE:</p> <ul style="list-style-type: none"> • Who is on the committee(s)/ what departments/ what level of seniority? What's their role? • How often do they discuss cyber issues? • What information do they receive? / Do they receive reports on cyber – how often? 	
<p>4. Corporate/external reporting</p>	<p>6-7 mins</p>
<p>Thank you very much for your answers so far. Moving on to talking about your annual reporting, in your most recent annual report, what kind of things did you include about your cyber security? PROBE ON:</p> <ul style="list-style-type: none"> • What governance processes are in place for managing cyber resilience • How the organisation assesses its cyber resilience • Type of cyber risk strategy <ul style="list-style-type: none"> - How often the strategy is reviewed - Whether you receive independent assurance of the strategy • How your organisation manages supply chain risk • How you ensure that responsibility for cyber resilience is embedded across the organisation • How often staff receive cyber security training • Anything else? <p>Why do you choose to include these things as opposed to others? (could give example of those not mentioned)</p> <p>Is there anything that I've just mentioned and you haven't included in your annual reports to date that you think would be useful to include going forward? Anything else?</p>	<p><i>This explores the type of information that organisations include in their reports on cyber security.</i></p>

<ul style="list-style-type: none"> ● IF YES: What's stopped you from including that information until now? ● IF NO: Why not? 	
<p>5a. Designated responsibility/oversight</p>	<p>5 mins</p>
<p>PRIORITY / IF HAVE TIME DEPENDING ON THE INTERVIEW</p> <p>The next few questions will be about how your board engages with cyber security.</p> <p>(Refer to survey answers Q_BOARDGOVERN)</p> <p>(If answered a1) In the survey you said that one or more board members roles include oversight of cyber security risks.</p> <ul style="list-style-type: none"> ● What does this role entail? ● Do board members understand your organisation's cyber security defences, and key cyber security threats? ● Are they responsible for approving or signing off on the organisations approach to cyber/cyber resilience strategy? Do they take a reactive approach (based on previous incidents) or a proactive approach (based on what they think cyber risks are going to be)? <p>(If answered b1) In the survey you said that you have a designated staff member responsible for cyber security, who reports directly to the board.</p> <ul style="list-style-type: none"> ● What does this role entail? ● Do they have the authority/influence to make decisions? ● Does the designated staff member understand your organisations cyber security defences, and key cyber security threats? <p>(If answered a1 and b1) How do the designated staff member and board member(s) responsible for cyber security work together, if at all?</p> <ul style="list-style-type: none"> ● How do they share information with each other? / How frequently? ● What information do they usually discuss? PROBE ON: <ul style="list-style-type: none"> - Cyber KPIs (key performance indicators) - Cyber news - Cyber projects/investment - Cyber risks in the business - Cyber threats/attacks 	<p><i>This section explores who in the organisation has responsibility for overseeing cyber security, what the role involves and how much authority they have to influence cyber security decisions.</i></p> <p><i>Please ask all questions that are relevant, for example, if the participant answered a1 and b1 ask all 3 questions.</i></p>

<ul style="list-style-type: none"> Do they generally discuss internal or external cyber threats? 	
<p>5b. Supply chains and external consultants</p>	<p>5-8 mins</p>
<p>PRIORITY / IF HAVE TIME DEPENDING ON THE INTERVIEW</p> <p>In the final few minutes, I would like to talk a bit about supply chains.</p> <p>Is cyber security considered as a risk when you choose a supplier? How does it influence/factor into your choices?</p> <ul style="list-style-type: none"> Who is responsible for managing the cyber security risks posed by your suppliers? What responsibility lies with the suppliers? What lies with your organisation? Why? Is cyber risk built into contracts? What impact does this have on the cyber measures you take with suppliers? PROBE ON: <ul style="list-style-type: none"> Impact of legal protection Greater knowledge/awareness What are the reasons behind investing in your supply chain risk management? <ul style="list-style-type: none"> Has your priority of investing in supply chain risk management changed over time? IF YES: Why? Does your organisation have a strategy in place to address cyber security threats that emerge from vulnerabilities in supply chains? How aware are you of which suppliers have access to your IT systems? How does it affect how you manage cyber security risks? How aware are you of which of your suppliers are essential to the continuity of your organisation? How does it affect how you manage cyber security risks? What role, if any, do the board play in supporting supply chain cyber risk management? <p>IF TIME ALLOWS</p> <p>Does your organisation currently use external IT or cyber security consultants?</p> <ul style="list-style-type: none"> IF NO: Probe to understand why not – lack of trust, too expensive etc. IF YES: <ul style="list-style-type: none"> Why did you decide to use external consultants? What do these consultants do? 	<p><i>This section explores how organisations manage the cyber security risks of their supply chain.</i></p>

Department for Digital, Culture, Media and Sport	
Cyber Security Longitudinal Survey Wave 1: Technical Annex	

<ul style="list-style-type: none"> • How did you choose the consultant? How much did you know about their services? • How much, if at all, would you say you trust these external consultants? 	
Wrap-up	2-3 mins
<p>Overall, what do you think I should take away from the discussion today?</p> <p>Is there anything you feel that we haven't covered today that you would like to share?</p> <p>Inform about next steps and incentive.</p> <p>THANK AND CLOSE</p>	<i>Wrap up the interview</i>

Appendix C: Further information

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.

- Allan Simpson, Ipsos MORI
- Aniko Lakezi, Ipsos MORI
- Iona Gallacher, Ipsos MORI
- Alex Bollen, Ipsos MORI
- Jayesh Navin Shah, Ipsos MORI
- Professor Steven Furnell, University of Nottingham.

The responsible DCMS analyst for this release is Maddy Ell. The responsible statistician is Robbie Gallucci (evidence@dcms.gov.uk).

For general enquiries contact:

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

Telephone: 020 7211 6000

DCMS statisticians can be followed on Twitter via [@DCMSInsight](https://twitter.com/DCMSInsight).

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