Department for Science, Innovation, & Technology

Ipsos

Cyber Security Longitudinal Survey Wave Three

Technical Annex

This Technical Annex provides details of the methodology of the Cyber Security Longitudinal Survey (CSLS) Wave Three. It covers the quantitative survey (fieldwork March – June 2023) and qualitative element (carried out in June - July 2023), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

This annex supplements a main Analytical Release and infographic summaries published by the Department for Science, Innovation and Technology (DSIT), covering the results for businesses and charities.

The Cyber Security Longitudinal Survey (CSLS) is a multi-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 third research year, and therefore the main objective of this report is to establish any significant trends that have occurred across the three years of the research. The quantitative survey was carried out in March-June 2023 and the qualitative element in June-July 2023.

Responsible analyst

Emma Johns

Enquiries:

cybersurveys@dsit.gov.uk

Table of Contents

Chapter 1: Overview

1.1 Summary of methodology

The Cyber Security Longitudinal Survey (CSLS) Wave Three pertains to the third year of a longitudinal research project.

For this study, we undertook a random probability multimode (telephone and online) survey of 542 UK businesses and 310 UK registered charities. The main stage survey took place between 27 March and 12 June 2023. The data for businesses and charities have been weighted to be statistically representative of these two populations.

In addition, we carried out 30 in-depth interviews in June and July 2023 to gain further qualitative insights from some of the organisations that answered the survey.

The longitudinal nature of the Wave Three survey means that we largely interviewed the same organisations as in Wave Two, but we also used a top-up sample to account for attrition or dropout (where our contact from the previous year was unable or unwilling to participate again, including having left the organisation or being on long-term leave).

Therefore, we focus the study on repeat observations with the same organisations where possible and replace any dropouts from the survey with fresh sample. This allows for better cross-sectional analysis, as it ensures a representative sample overall each wave. This approach also adds flexibility to the longitudinal analysis as there is no hard requirement for organisations to take part in all three waves.

This design enables the following key long-term objectives of this research to be met:

- to explore how and why UK organisations are changing their cyber security profile and how they implement, measure, and improve their cyber defences
- to provide a more in-depth picture of larger organisations, exploring topics that are covered in less detail 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
- to explore the effect of actions adopted by organisations to improve their cyber security to the likelihood and impact of a cyber security incident

The scope of this survey covers medium (defined as 50-249 employees) and large (defined as 250+ employees) businesses and high-income charities (defined as a turnover of at least £1 million). If organisations had been confirmed as eligible and interviewed in an earlier wave but now have fewer than 50 employees (businesses) or a turnover of less than £1 million (charities), they were still considered eligible to be interviewed – this applied to 17 businesses in Wave Three.

Businesses with fewer than 50 employees, charities with a turnover lower than £1 million, and all public-sector organisations were outside the scope of the survey and therefore excluded from the top-up sample. 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 Strategy 2022.

This study differs from the CSBS in several important respects:

- 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.
- 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 charities and educational institutions. Therefore, while there are some similarities in the questions and topics covered by the two surveys, results are not comparable due to the differing survey designs and methodologies
- 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	Has your organisation carried out any work to formally review the following?: A) The potential cyber security risks presented by your immediate suppliers [IF CHARITY/EDUCATION: or partners] B) The potential cyber security risks presented by your wider supply chain, i.e. your suppliers' suppliers
Q_DISRUPTA	What kind of breach 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 breaches or attacks impacted your organisation in any of the following ways, or not?

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

To see publications of the CSBS, please visit the gov.uk website.

1.3 Benefits and limitations of the survey

CSLS provides longitudinal analysis and 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 CSLS are:

- The use of random probability sampling to minimise selection bias a multimode survey including a telephone data collection approach, which aims to also include businesses and charities with limited 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).
- As a 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 a cyber security 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 relatively low with most organisations taking part (c.80%) indicating they are happy to participate in future years, with around half of those participating in the following year.
- Organisations can only tell us about the cyber security incidents that they have detected. There may be other cyber security 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 tend to systematically underestimate the real level of cyber security incidents.

- 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 CSBS 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 cyber security incidents. Again, this implies that respondents may underestimate the total cost of all cyber security incidents (including undetected ones).

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

Ipsos developed the questionnaire and all other survey instruments (e.g., the interview script and briefing materials) and DSIT had final approval of the questionnaire.

In Wave One of the survey the Ipsos research team carried out cognitive testing interviews with businesses and charities to test comprehension of the questions. Waves One and Two of the survey also included a three-day pilot stage, in which new questions could be tested for comprehension and questionnaire length could be monitored. Cognitive testing and piloting were not considered necessary for Wave Three due to the limited number of changes from the Wave Two questionnaire.

Changes to the questionnaire between Wave One and Wave Two were as follows:

- **Q_CHARITYINCOME.** This question was added to obtain slightly more granular data on charity income than the previous simple confirmation of income being £1 million+ per annum in Wave One
- **Q_BOARDTRAINFREQ.** This was added in Wave Two as a follow-up to the existing yes/no question on whether any of the board had received cyber security training, that asks how often the board receives cyber security training

Questionnaire development for Wave Three of the survey was limited to the amendment of pre-existing questions, for maximum comparability between waves of the survey. The amendments made were:

- **Q_RULES.** One code (‘any monitoring of user activity’) was amended to add a brief clarification (‘i.e., not network monitoring’)
- **Q_COMPLY**. Scripting was amended at this question so that respondents could not answer both code 2 (The Cyber Essentials Standard) and code 3 (The Cyber Essentials Plus Standard)
- **Q_GUIDANCE.** Three codes were removed and four were introduced for this question. Codes removed were: Guidance on secure home working or video conferencing; Guidance for moving your business online; and Cyber Readiness Tool. Codes introduced were: Ransomware guidance; Exercise in a box; Device security guidance; and Early warning service.

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 Computer-Assisted Telephone Interviewing (CATI) script (e.g., to organisations that wanted more information) also included a link to the GOV.UK page.

2.3 Sampling

The sample for Wave Three of the survey was split between two types: panel and fresh sample.

Panel sample

Wave Three of the CSLS was focused on repeat observations with the same organisations that had been interviewed in Wave Two of the survey. Therefore, much of the sample was 'panel sample', meaning respondents who had been interviewed in Wave One and Wave Two of the survey.

After those who had not given permission to be re-contacted for Wave Three had been excluded, there were 899 cases within the panel sample, comprised of 599 businesses and 300 charities. A breakdown of the 599 businesses by size and sector is shown in Table 2.1 below.

Table 2.1 Issued panel business 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	1	1	0	2
C	Manufacturing	66	29	11	106
F	Construction	27	7	6	40
G	Retail or wholesale (including vehicle sales and repairs)	54	18	10	82
H	Transport or storage	17	8	7	32
I	Food or hospitality	29	14	11	54
J	Information or communication	34	4	3	41
K	Finance or insurance	18	4	4	26
L	Real estate	3	1	1	5
M	Professional, scientific, or technical	29	3	3	35
N	Administration	28	24	30	82
P	Education (excluding public sector schools, colleges, and universities)	5	6	10	21
Q	Health, social care, or social work (excluding NHS)	24	19	9	52
R	Arts or recreation	8	4	3	15
S	Service or membership organisations	3	2	1	6
Total		**346**	**144**	**109**	**599**

Across each of the waves, the size of the panel falls due to attrition to each wave:

Table 2.2 Panel attrition across all three waves

	Wave 1	**Wave 2**	**Wave 3**
Total completed interviews	1741	1061	852
Panel interviews	-	674	451
Cross sectional interviews	1741	387	401
Agree to be in panel sample	1405	899	724
Retention rate	81%	85%	85%
Attrition rate	19%	15%	15%

Only 316 organisations have taken part in the survey across all three waves.

To replace dropouts from the survey, top-up sample is also used. The rest of this chapter refers to this fresh sample.

Business population and sample frame

The target population of this research is medium and large businesses. This is because these businesses are 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 year one of this research in 2020, similar proportions of medium and large businesses experienced cyber security incidents within the last 12 months, and both reported 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 population[1] of 35,900 according to the latest Business Population Estimates).
- large businesses with 250+ staff (a population of 7,700 according to the latest 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

Aside from 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.

Organisations in the agriculture, forestry, and fishing sectors (SIC 2007 category A) were also excluded. At the time of Wave One of this survey, this was in line with other cyber security surveys such as the CSBS, which excluded these sectors due to practical considerations as well as a perceived lack of relevance to cyber security. Due to the longitudinal nature of this survey and the sample, these sectors continue to be excluded in Wave Three.

Further to this, the IDBR contains some organisations that are defined as being in the 'not-for-profit' sector. This included a range of organisation types, such as religious institutions and

[1] 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.

educational establishments. As the IDBR sample was intended to act as a top-up for businesses, these organisations fell outside the definition of a business for this wave.

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 9,755 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 (OSCR) 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. DSIT 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 in the last few years. Alternative sample frames for Northern Ireland, such as the Experian and Dun & Bradstreet business directories (which also include charities), were 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. As only eight Northern Ireland-based charities were interviewed, this is too small a base size for undertaking sub-group analysis.

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

- charities with 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, 49,765 ‘fresh’ businesses were selected from the latest available version of IDBR as potentially eligible for the survey.[2]

We determined this to be an accurate population based on previous successful sampling for CSBS, along with Waves One and Two of the CSLS. The principal challenge considered was to mitigate against the risk of varying sample quality experienced in similar surveys in recent years

[2] Please note, this is the raw unclean count and as such differs from the business population statistics.

(in terms of telephone coverage and usable leads). 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 the majority of a random non-small business sample to be medium businesses. Hence, the sample of large 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, 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 2.3 breaks down the selected business sample by size and sector.

Table 2.3 Fresh business sample by size and sector (raw data pre-cleaning)

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	380	69	76	525
C	Manufacturing	6,187	778	595	7,560
F	Construction	2,133	159	148	2,440
G	Retail or wholesale (including vehicle sales and repairs)	5,294	583	622	6,499
H	Transport or storage	1,632	176	189	1,997
I	Food or hospitality	3,259	327	340	3,926
J	Information or communication	2,460	278	235	2,973
K	Finance or insurance	1,045	184	246	1,475
L	Real estate	542	107	115	764
M	Professional, scientific, or technical	4,086	453	421	4,960

N	Administration	4,374	618	599	5,591
P	Education (excluding public sector schools, colleges, and universities)	1,522	327	356	2205
Q	Health, social care, or social work (excluding NHS)	5,479	496	433	6,408
R	Arts or recreation	1279	159	142	1,580
S	Service or membership organisations	737	66	57	860
Total		40,409	4,780	4,575	49,764

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) due to 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. As stated above, 9,755 leads were received from the relevant charity regulators (i.e., 9,455 charities when the 300 charities in the panel sample are excluded).

Sample data cleaning

Not all the original sample was usable. Checks were undertaken for the following:

- missing or invalid telephone numbers (i.e., the number was either in an incorrect format, too long, too short, had an invalid string, or a number which would charge the respondent when called)
- duplicated records
- against our central ‘do not contact’ list of organisations (i.e., those who have explicitly asked to be removed from any contact from Ipsos across any/all surveys)
- Wave Two participants that did not give consent to be re-contacted for Wave Three, and organisations that took part in the CSBS 2023

Table 2.4 breaks down the usable fresh business sample by size and sector, a total of 34,539 fresh business leads remained post-cleaning, in addition to 9,524 charities.

Table 2.4 Fresh business sample by size and sector (post-cleaning)

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	302	55	58	415
C	Manufacturing	5,111	629	462	6,202
F	Construction	1,753	120	127	2,000
G	Retail or wholesale (including vehicle sales and repairs)	4,141	482	467	5,090
H	Transport or storage	1,293	143	149	1,585
I	Food or hospitality	2,180	246	280	2,706
J	Information or communication	1,595	182	164	1,941
K	Finance or insurance	802	144	199	1,145
L	Real estate	345	60	66	471
M	Professional, scientific, or technical	936	345	304	3,585
N	Administration	3,009	468	449	3,926
P	Education (excluding public sector schools, colleges, and universities)	553	64	47	664
Q	Health, social care, or social work (excluding NHS)	3,300	230	181	3,711
R	Arts or recreation	631	93	83	807
S	Service or membership organisations	252	21	18	291
Total		28,203	3,282	3,054	34,539

Sample batches

For businesses and charities, the usable sample for the main stage survey was randomly allocated into separate batches. The initial batch was the 899 records from the panel sample, which were fielded all at once.

The second batch of sample was the fresh charity sample. This was based on a simple random selection of 1,001 charities from the cleaned sample. This sample was then fully worked to top up the charity panel.

Subsequently, the business sample batches were released. For the fresh business sample, the approximate of the sample required to achieve the target number of completed interviews was calculated before being drawn into batches.

The first fresh business sample batch had 1,910 records and the second contained 1,895 cases. The third and fourth batches each contained 382 records. These batches were selected using a stratified disproportionate random approach. Owing to both the expected difficulty in

contacting the largest businesses and to the differential response rates by sector, more large/very large businesses were selected. These were then allocated to the highest priority sectors, to ensure these sample cases were given sufficient time in field.

Across all sample groups, six batches of sample were released throughout fieldwork. We aimed to maximise the response rate by fully exhausting the existing sample batches before releasing additional records. This aim was balanced against the need to meet interview targets, particularly for boosted sample groups (without setting specific interview quotas). A total of 6,469 fresh sample leads were released (5,168 businesses and 1,301 charities).

2.4 Fieldwork

Ipsos carried out fieldwork between 27 March and 12 June 2023 using a Computer-Assisted Telephone Interviewing (CATI) option and an online survey option.

In total we completed 852 interviews with:

- 542 businesses
- 310 charities

The average interview length was c.25 minutes for all groups. This was generally in line with the second wave of the survey.

Most interviews were with repeat organisations from previous waves of the survey of the survey.

- 451 were from the panel sample (280 businesses, 171 charities)
- 401 were from the fresh sample (262 businesses, 139 charities)

Fieldwork preparation

Prior to fieldwork, the Ipsos 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 (fresh sample)

Interviewers screened all fresh sample at the beginning of the call to identify the right individual to take part and to ensure the organisation was eligible for the survey. At this point, the following organisations in the fresh sample were removed as ineligible:

- businesses with fewer than 50 employees
- charities with an income lower than £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 £1 million or higher) were included as charities and asked the survey questions on this basis. In

total, 8 organisations that 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

For the fresh sample, 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:

- Each organisation loaded was called either a minimum of 7 times (10 times for panel sample) or until an interview was achieved, a refusal was given, or information was obtained to make a judgement 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.
- An online version of the survey was available. Sample contacts with known email addresses were sent unique links to the online survey in a series of reminder emails.

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 set up an email inbox and free (0800) phone number for respondents to be able to make contact to set up appointments or, in case they have contacted Ipsos by phone, 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 interviewer would attempt to call them. These were sent to 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 was genuine. The web pages included appropriate Privacy Notices on the processing of personal data, and the data rights of participants, in line with UK GDPR.
- The survey was endorsed by the National Cyber Security Centre (NCSC), the Home Office, the Scottish Government, 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 large businesses, Ipsos offered a £10 charity donation as a thank you for their time.
- Additionally, to maximise the response rate among the panel, and minimise the potential for attrition bias, the panel sample were initially contacted via email to "warm up" the sample before the CATI fieldwork began. Furthermore, to best take advantage of this initial contact process, the panel sample was the first sample to be called during the CATI fieldwork.

Online completion option

To boost response rates and reflect increasing preference for online survey options, an online completion option was again included. Sample records with email addresses were sent an online link to the survey if requested during a telephone interview. A majority of completed interviews were still completed by telephone.

- 786 interviews (92.3%) were completed through the CATI option
- 66 interviews (7.7%) were completed through the online option

Fieldwork monitoring

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

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 2.5 shows the final outcomes and the adjusted response rate calculations for businesses and charities.[3]

[3] 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.

Table 2.5: Fieldwork outcomes and response rate calculations for businesses and charities (by sample type)

Outcome	Businesses fresh sample	Charities fresh sample	Businesses panel sample	Charities panel sample
Total sample loaded	4,569	1,001	599	300
Completed interviews	262	139	280	171
Incomplete interviews	46	25	9	0
Unusable leads	1,207	172	54	31
Ineligible leads – established during screener [4[1]]	65	41	6	2
Refusals [5[2]]	547	154	54	20

Response rates and expected negligible impact on the survey's reliability

Half of the available panel sample (451 out of 899 leads, or 50%) took part again in this wave, including 57% of charities and 47% of businesses, which was in line with expectations. In total, 316 organisations took part in all three waves.

The adjusted fresh sample response rates[6] for businesses (8%) and charities (18%) are broadly similar to the overall response rates observed in CSBS 2023 (7% for businesses and 13% for charities), and in line with both CSBS and CSLS in 2022.

The low response rates compared to pre-2020 business surveys are likely to be due to a combination of circumstances, including:

- the hybrid working conditions adopted by many organisations since the pandemic
- the ongoing challenge of declining response rates in telephone survey fieldwork in general, including in business surveys specifically.

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

The effects of hybrid working proved especially challenging, due to various factors:

4[1] 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.

5[2] 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.

6 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. The assumed eligibility rate for the refusals was 90%.

- it is hard to reach organisations via landline numbers given the embedding of video conferencing in working practices.
- when we do get through, it is harder to reach the right individual within the organisation, who may have been working remotely rather than in an office
- where we do reach the right person, these individuals are often busy due to the overall strain that hybrid working has placed on IT and cyber teams and therefore these teams remain less willing to take part in surveys in general

Furthermore, the increase in the survey length from c.22 minutes in the first wave of the survey, to c.25 minutes in Waves Two and Three will have reduced the response rate – interviewers must mention the average length to respondents when they introduce the survey, and respondents are naturally less inclined to take part in longer interviews.

To a lesser extent, continuing business and charity participation in the CSBS may impact the performance of this survey. Organisations that took part in the CSBS were excluded from the sample for this survey. However, organisations that were contacted for CSBS but opted not to take part may also have been resampled and contacted anew for this survey and been less likely to take part as a result.

However, it is important to remember that response rates are not a direct measure of non-response bias in a survey, but only a measure of the potential for non-response bias to exist. Previous research into response rates, mainly with consumer surveys, has indicated that they are often poorly correlated with non-response bias.[7] We have no reason to assume that the organisations declining to take part are systematically different in terms of their cyber security approaches to the ones we did interview. It is also possible for the composition of the panel sample to change over time as some organisations drop out of the sample. Response rates among the panel were maximised, which helped to ensure that the retention rate was high and as a result ensure that attrition bias was mitigated as much as possible.

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 cyber security 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. A test exercise in 2017 overwhelmingly found the SIC 2007 codes in the sample to be accurate, so this practice was carried forward to subsequent surveys.

[7] 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).

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). 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 applied RIM weighting to the business sample for two key reasons. Firstly, to account for the natural variability between the sample and the population data as much as 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.

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 2022.

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.

All weighting is fully consistent with the previous waves of the survey. Longitudinal weights are not required and therefore not in the accompanying public dataset but will be applied for any discrete analysis of the longitudinal sample.

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

Table 2.6: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %[8]
Size		
Medium (50–249 staff)	58.4%[9]	82.3%
Large (250-499 staff)	18.5%	8.9%
Very large (500+ staff)	22.7%	8.7%
SIC / Sector		
B/D/E: Utilities or production	0.4%	1.5%
C: Manufacturing	21.0%	17.0%
F: Construction	7.7%	5.5%
G: Retail or wholesale (including vehicle sales and repairs)	13.5%	14.6%
H: Transport or storage	4.2%	4.4%
I: Food or hospitality	10.3%	8.3%
J: Information or communication	5.7%	6.3%
K: Finance or insurance	2.8%	3.1%
M: Professional, scientific, or technical	5.4%	10.5%
N/L: Administration or real estate	16.4%	13.7%
P: Education (excluding public sector schools, colleges, and universities)	2.9%	1.8%
Q: Health, social care, or social work (excluding NHS)	7.4%	10.1%
R/S: Entertainment, service or membership organisations	2.2%	3.3%

2.7 SPSS data uploaded to UK Data Archive

Derived variables

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

We agreed with DSIT from the outset of the first wave of the survey that for those who gave banded responses, a numeric response would be imputed in line with the approach taken in the

[8] All percentages shown here are rounded to 1 place, and are subsequently re-based so that charities are weighted to reflect their share of the total sample (charities 35.156%, businesses 64.844%)

[9] Includes 17 interviews with panel businesses that had 50-249 employees when first interviewed (in 2021 or 2022), but fewer than 50 employees in 2023 - these were therefore still considered eligible.

CSBS. 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 one most disruptive incident being collected in four constituent questions, and the overall financial cost of all cyber security incidents 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 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 cyber security 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 cyber security incidents to organisations.

To run the calculations for the derived variable, DSIT and Ipsos 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 cyber security 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 2.7 below.

Table 2.7: Derived combined cost of most disruptive incident vs. overall cost of all cyber security 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	£1,840	£2,718	£1,159	£2,192	£4,911	£4,993	£843	£2,583
Median cost	£50	£100	£50	£100	£85	£206	£59	£150
Base	398	389	214	212	173	166	234	232
	Only across organisations identifying incidents with an outcome							
Mean cost	£5,991	£7,187	£3,650	£5,480	£13,532	£12,273	£2,598	£6,932
Median cost	£500	£1,500	£500	£1,500	£500	£1,000	£525	£1,000
Base	99	95	49	48	50	46	56	54

This discrepancy between the mean and median figures may be the result of outliers in the dataset affecting the mean but not the median, as well as:

- 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

As in previous waves, no numeric £ variables were included in the published SPSS dataset. This was agreed with DSIT 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 (damagedirlx_bands)
- the estimated staffing cost (damagestaffx_bands)
- the estimated damage or disruption cost (damagelindx_bands)
- the estimated cost of all cyber security incidents identified in the last 12 months (cost_bands)

Rounding differences between the SPSS dataset and published data

If running analysis on weighted data in SPSS, users must be aware that the default setting of the SPSS crosstabs command does not handle non-integer weighting in the same way as typical survey data tables.[10] Users may, therefore, see very minor differences in results between the SPSS dataset and the percentages in the main release and infographics, which consistently use the survey data tables. These should be differences of no more than one percentage point, and only occur on rare occasions.

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

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, 438 respondents (51%), including 269 businesses (50%) and 169 charities (55%), agreed to be recontacted. Organisations that took part in the qualitative follow-up stage of previous waves of the survey were not eligible to take part in the qualitative follow-up stage in this wave. Therefore, 24 organisations (16 businesses and 8 charities) were removed from the final sample for qualitative fieldwork.

We carried out interviews with 20 businesses and 10 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 £60 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.

Fieldwork

The Ipsos research team carried out all fieldwork in June and July 2023. We conducted the 30 interviews through a mix of telephone and Microsoft Teams calls. Interviews lasted around 45-50 minutes on average.

DSIT originally laid out their topics of interest for these interviews in 2021. Ipsos then revisited the original topic guide with DSIT in both 2022 and 2023. This resulted in a slightly updated guide with DSIT's guidance as to existing and new topics to be included. The topic guide for the third wave of the survey was broadly in line with the topic guide for the second wave, with an additional focus on whether organisations feel they are making progress with their cyber security processes, and the use of Cyber Essentials in supply chain risk management. The final topic guide was reviewed and approved by DSIT. 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?
- Does your organisation adhere to the Cyber Essentials standard? Why/ Why not?

- 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?

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

Tables 3.1 and 3.2 show a profile of the 20 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)	6
F	Construction	2
G	Retail or wholesale (including vehicle sales and repairs)	1
H	Transport or storage	1
I	Food or hospitality	2
J	Information or communications	3
K	Finance or insurance	0
L, N	Administration or real estate	1
M	Professional, scientific or technical	0
P	Education (excluding state education institutions)	2
Q	Health, social care or social work	1
R, S	Entertainment, service or membership organisations	1
	Total	**20**

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)	8

3.2 Analysis

Throughout fieldwork, the core research team discussed interim findings. We held two analysis meetings over MS Teams with the fieldwork team – one halfway through fieldwork and one at 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 relevant research questions. The research team reviewed these notes and listened back to recordings 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, DSIT is committed to monitoring and reducing the burden on those providing their information and on those involved in collecting, recording, and supplying data. Ipsos also consulted and complied with Government Social Research (GSR) guidelines on ethics.

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 **852 respondents** and the average (mean) survey length was **25 minutes**. Therefore, the research compliance cost for the quantitative survey this year was [852 × 25 minutes = **355 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 CSLS Wave Three was **380 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.

Chapter 5: Longitudinal analysis

Data preparation

As noted earlier in this document, three waves of the survey have been conducted. The second wave of the CSLS comprises interviews both with those that have completed the Wave One survey and an additional fresh sample of organisations providing their first interviews at Wave Two. Wave Three also continues this pattern by following up Wave Two interviewees and adding in a new cohort of fresh organisations. Table 5.1 outlines how each of these sample types breaks down across waves.

Table 5.1: Profile of respondents by wave

Sample type	Wave 1	Wave 2	Wave 3
Cross-sectional	1741	1061	852
Panel sample	N/A	674	451
All three waves	N/A	N/A	316

For the descriptive analysis presented in the main report, we combined the 674 cases responding to both Waves One and Two with the 451 cases responding to both Waves Two and Three into a single dataset. This gave 1,125 wave-on-wave transitions to observe. A drawback of this approach is that those cases appearing in all three waves are double counted, so we make no attempt here to weight back to the original sample of organisations. However, the benefit of this approach is that it provides a more detailed insight into stability transitions than would be possible if treating each pair of waves separately.

Segmentation

A latent class analysis (LCA) procedure, using Proc LCA in SAS 9.4, was used to explore segmentation solutions for the variables described in Table 5.2. LCA is a statistical technique that groups respondents together into classes where each member of the class has a similar response pattern across all the variables used to build the model. Each of the variables was coded as binary, with missing values recoded to ‘No’. This avoids issues of reduced sample size resulting from excluding cases with missing values from the analysis. Consequently, the percentage that answer positively is based on those that definitively report the presence of the relevant item (e.g., a cyber security vulnerability audit).

The segmentation aimed to explore a range of cyber resilience practices including:

- activities undertaken in the last 12 months to identify cyber security risks
- board involvement in cyber security
- risk governance around cyber security
- rules for storing, moving and accessing data
- improvements made in technical security over the last 12 months and assessment or management of supplier risk in last 12 months

A set of questions covering these cyber security practices were initially identified and reviewed for suitability of inclusion. A number of questions were excluded because of high percentage

agreement rates between segmentation groups. Given nearly all organisations reported undertaking them, the inclusion of these questions would have prevented us from separating cases into distinct latent classes.

Table 5.2: Variables considered for segmentation

Question included in Segmentation Model	Percentage that answer positively to each question
A cyber security vulnerability audit	50%
A risk assessment covering cyber security risks	69%
Invested in threat intelligence	35%
Used specific tools designed for security monitoring, such as Intrusion Detection Systems	63%
A policy to apply software security updates within 14 days	64%
Any monitoring of user activity	66%
Backing up data securely via a cloud service	75%
Backing up data securely via other means	69%
A Business Continuity Plan that covers cyber security	71%
A risk register that covers cyber security	57%
Any documentation that outlines how much cyber risk your organisation is willing to accept	29%
Any documentation that identifies the most critical assets that your organisation wants to protect	58%
A written list of your organisation's IT estate and vulnerabilities	57%
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	26%
Your processes for updating and patching systems and software	49%
Your processes for managing cyber security incidents	44%
Your malware defences	56%
Your processes for user authentication and access control	61%
The way you monitor systems or network traffic	46%
Your network security	65%
One or more board members whose roles include oversight of cyber security risks	48%
A designated staff member responsible for cyber security, who reports directly to the board	58%

Question excluded from Segmentation Model	Percentage that answer positively to each question
A cloud server that stores your data or files	72%
Your own physical server that stores your data or files	79%
A virtual private network, or VPN, for staff connecting remotely	73%
Specific rules for storing and moving files containing people's personal data	86%
Up-to-date malware protection across all your devices	96%
Firewalls that cover your entire IT network, as well as individual devices	94%
Restricting IT admin and access rights to specific users	96%
Security controls on your organisation's own devices (e.g. laptops)	93%

There is no fixed rule to produce the number of latent classes underlying the statistical associations between the variables. To determine a suitable course of action, models were run including consecutive numbers between two and six latent classes, each of which included the 22 items described in Table 5.2. While statistical measures exist (e.g., measures of entropy[11]) and can be used to determine goodness of fit, these are not always conclusive. Therefore, we used entropy as a guide but based our selection of the final model on substantive considerations about the interpretability of the solutions and stability across evolutions as the numbers of classes increased.

The key gain from moving from a four to a five-class solution arises from the formation of the Mostly class, forming largely from the Technical class and the High class. The Technical class also makes gains from the Low class. The solution is otherwise relatively stable (Table 5.3).

[11] Entropy is a measure of how well the LCA solution separates organisations into unique classes. Higher entropy denotes a better degree of separation, i.e., organisations can be more definitively assigned to one class rather than another. However, high entropy also occurs with an over-fit model so we do not use it as a definitive measure for model selection.

Table 5.3: Evolution of the four-five class solution

Classes	1	2	3	4	Total
1 (Governance)	308	7	14	1	330
2 (Technical)	4	186	73	0	263
3 (Low)	0	0	270	0	270
4 (High)	0	0	0	355	355
5 (Mostly)	24	316	0	183	523
Total	336	509	357	539	1741

The addition of a sixth class was an eclectic mix of Governance, High and Mostly and resulted in a relatively small number of cases in this class (Table 5.4). The stability of this relatively small class size over time, i.e., after attrition at Waves Two and Three, along with the challenge of understanding how it differed substantially from the Governance, High and Mostly classes meant that we decided upon the five-class solution presented in the main report. As is shown in the main report, a five-class solution provides an interpretable segmentation, which is stable across time.

Table 5.4: Evolution of the five-six class solution

Classes	1 (Gov)	2 (Tech)	3 (Low)	4 (High)	5 (Mostly)	Total
1	227	30	56	0	0	313
2	0	220	0	0	0	220
3	0	2	214	0	0	216
4	0	0	0	306	13	319
5	4	11	0	9	480	504
6	99	0	0	40	30	169
Total	330	263	270	355	523	1741

Having reviewed the different options, it was decided that a five-class solution was the most appropriate segmentation for this data. These five segments were then given names to ensure that it was clear what each segment referred to in practice:

- **Low cyber security protection:** for these organisations, protection was low across all activities, except secure cloud backup. On average, organisations had completed 4 cyber security activities.
- **Technical led cyber security protection:** these organisations tended to have had recent improvements in network security, malware defence, authentication and secure backup but lower than average governance. On average, organisations had completed 9 cyber security activities.

- **Governance led cyber security protection:** for these organisations, protection was around or above average for policy and procedures but low on technical responses. On average, organisations had completed 11 cyber security activities.
- **Mostly prepared cyber security:** these organisations had mostly above average protection on all items but to a lesser extent than those in the 'high' level group. On average, organisations had completed 15 cyber security activities.
- **High cyber security protection:** for these organisations, protection was well above the average level on all activities. On average, organisations had completed 19 cyber security activities.

A discriminant function analysis (DFA) was undertaken, using Proc Discrim in SAS 9.4, where the 22 variables from which the model is comprised (as shown in Table 5.2) were used to predict the latent classes. DFA is a statistical technique that uses a set of variables to predict known group membership. This model was used to predict segment group membership at Waves Two and Three.

After the segmentation was modelled for Waves Two and Three, the data was restructured to into two time periods: pre-wave and post-wave. For respondents who completed their interviews in Wave One and Two, Wave One acted as the pre-wave and Wave Two acted as the post-wave. For respondents who completed in Wave Two and Three, Wave Two acted as the pre-wave and Wave Three acted as the post-wave. For respondents that participated in all three waves, the analysis included these organisations twice, following the same scheme as outlined above. Once this restructuring was completed, the analysis was completed by testing how the pre-wave data had changed in the post-wave.

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

Q_CHARITYINCOME

ASK IF CHARITY (CODE 2 AT Q_TYPEDUM)

In the last financial year, was the annual income of your charity…?

CATI: READ OUT – RESPONDENT'S BEST GUESS IS FINE.

SINGLE CODE

1. Less than £1 million [CLOSE SURVEY EXCEPT IF PANEL RE-CONTACT SAMPLE]
2. £1 million but less than £3 million
3. £3 million or more
4. CATI: DO NOT READ OUT: Don't know
5. CATI: DO NOT READ OUT: Prefer not to say

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 EXCEPT IF PANEL RE-CONTACT SAMPLE]
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 EXCEPT IF PANEL RE-CONTACT SAMPLE]
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 EXCEPT IF PANEL RE-CONTACT SAMPLE]

Q_SIZEDUM

DUMMY VARIABLE NOT ASKED

MERGE RESPONSES FROM SIZEA AND SIZEB – IF PANEL SAMPLE AND UNDER 50 OR DON'T KNOW THEN CODE 1

SINGLE CODE

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

[Q_INCOME REMOVED AND REPLACED BY Q_CHARITYINCOME ABOVE]

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

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 (i.e. not network monitoring)
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 CODES 1-3 BUT KEEP CODES 2/3 TOGETHER

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

CATI: READ OUT

MULTICODE. CODE 2 OR 3 SET SO THEY CANNOT BE SELECTED TOGETHER

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

NOT PART OF ROTATION

4. CATI: DO NOT READ OUT [SINGLE CODE]: None of these
5. CATI: DO NOT READ OUT [SINGLE CODE]: 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

Q_BOARDTRAINFREQ

ASK IF BOARD HAS RECEIVED CYBER SECURITY TRAINING (BOARDTRAIN CODE 1)

On average, how often does the board receive cyber security training?

SINGLE CODE

1. Several times a year
2. Around once a year
3. Less often than once a year
4. Only received once / one-off training
5. CATI: DO NOT READ OUT: Don't know
6. CATI: DO NOT READ OUT: Prefer not to say

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 NCSC information or guidance, if any, have you used?

CATI: READ OUT

MULTICODE

1. Weekly threat reports
2. The 10 Steps to Cyber Security
3. Cyber Security Board Toolkit
4. Cyber Assessment Framework
5. GDPR guidance
6. Supply chain security guidance
7. Ransomware guidance
8. Exercise in a box
9. Device security guidance
10. Early warning service

SINGLE CODE

10. CATI: DO NOT READ OUT: None of these
11. 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 INCIDENTa-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 INCIDENTa-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 INCIDENTa-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. 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, and we will only report on aggregated findings and banded values, meaning that your organisation will not be identifiable based on your answers.

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 & 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

DSIT may 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 to contact you on behalf of DSIT for your views on this topic again within the next 18 months?

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

SINGLE CODE

1. Yes
2. No

Q_DCMSRECON

ASK ALL

Ipsos expects to undertake other research on the topic of cyber security on behalf of DSIT within the next 12 months. In these research studies, we would again randomly sample organisations in your sector and your organisation may be selected. In this case, having your individual contact details would save us from having to contact your switchboard. Would you be happy for us to securely hold your individual contact details for this purpose until July 2024 before securely deleting them? Participation in any other studies would still be voluntary.

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 £60 for their time. Would you be happy to receive an invite for one of these conversations in summer 2023, 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_NAME2

ASK IF PANELRECON CODE 1 AND Q_NAME NOT CODE 1

In case you are not available, please could we take a back-up name and job title?

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_DATALINK

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

Would it be possible for DSIT 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. Any data linked up to that point will remain, but no future linking will take place. Data will only be used to inform DSIT 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 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**
Introduction	**2-3 minutes**
● Introduce yourself and Ipsos – independent research organisation (i.e. independent of government) ● Commissioned by the Department for Science, Innovation and Technology (DSIT) ● 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 £60 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 GDPR consent (once recorder is on): ● Ipsos's legal basis for processing is your consent to take part in this research. ● Your participation in this research is voluntary. ● You can withdraw consent for data to be used at any point during or after the interview. Can I check you are happy to proceed?	*The welcome helps to orientate the participant and gets them prepared to take part in the interview.* *Outlines the "rules" of the interview (including those we are required to tell them about under MRS guidelines). This includes GDPR-related consent.* *Make this very brief – we have already spoken to these individuals in the survey, so they should understand the background.*

Context	**2 minutes**
Before we begin, could you briefly describe your day-to day role and the organisation you currently work for? 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?	*This section provides context to follow up on later in the interview, in terms of who is in charge and what they see as the risks.* *Make this very brief.*
1. Cyber security resilience	**13 minutes**
Thank you very much for your answers so far, the first section of our interview will focus on cyber resilience. **Do you feel that your organisation has appropriate controls and processes in place to mitigate against cyber 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* ● **And do you feel that these cyber controls and processes are improving, or getting worse over time?** ● *Probe on challenges organisations face around maintaining their cyber security practices* **Does your organisation have any cyber security measures in place to manage risk?** ● Why did you introduce these measures? IF NOT MENTIONED: Do you feel that having these cyber security measures in place gives	*This section explores the processes an organisation has in place to mitigate against, and recover from, cyber security incidents – whether they face any challenges in doing so and whether they think their level of investment is appropriate.*

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, **NCSC Cyber Security Toolkit**) ● How useful did you find this information? - IF USEFUL: What did you find particularly helpful? - 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)* - *Probe on whether they have clear roles and responsibilities that address cyber resilience as an organisation wide risk*	

- *Probe on whether they think they are given adequate resources, expertise and investment to enhance the organisation's cyber resilience.* ● **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? - Are senior leaders/the board involved – how? - Does the plan align with the organisation's continuity plan ● 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. Cyber Essentials	**3-4 minutes**
Now, I'd like to spend a couple of minutes talking about any standards or certifications your organisation may have. Is your organisation either ISO 27001 or Cyber Essentials certified? ASK ALL WHO ARE CYBER ESSENTIALS CERTIFIED **In the survey you said that your organisation is Cyber Essentials certified.** Why did your organisation choose to apply for this specific certification? What are the benefits of Cyber Essentials certification? How do these differ compared to other standards or certifications? Does your organisation use Cyber Essentials as a tool in managing and/ or assessing possible third-party cyber security risk? ASK ALL WHO ARE NOT CYBER ESSENTIALS CERTIFIED (OR DON'T KNOW) **Why are you not Cyber Essentials certified? (PROBE FULLY)** *If participants mentions that they adhere to CE controls without being certified, probe on this further.* Does your organisation use any other standards or certifications? IF YES: Why did your organisation choose this type of certification and not Cyber Essentials? What are the benefits of this accreditation? IF NO: Why not? (PROBE FULLY)	*This section explores the reasons why certain organisations chose to adhere to Cyber Essentials and why others do not.* ***For info*** *Cyber Essentials is a UK government information assurance scheme operated by the National Cyber Security Centre (NCSC), designed to show an organisation has a minimum level of protection in cyber security through annual assessments.* *Third party cyber risk is the potential threat presented to an organisations' internal sensitive information (e.g., employee/ customer or client data, financial information etc.) from the organisation's supply-chain and other outside parties that provide products and/or services that have access to internal systems.*
3. Internal reporting of cyber incidents	**7-8 minutes**

In the next few minutes, I would like to move on to talk about the way the board and/or committee of your organisation engages with cyber security incidents. ASK ALL **What types of internal reports, if any, does your board receive on cyber security?** ASK ALL WHO REPORT INTERNALLY TO BOARD ● 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? ASK ALL WHO DON'T REPORT INTERNALLY TO BOARD ● What are the reasons for not reporting information related to cyber security to the board? - 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? **Does your organisation have a Chief Information Security Officer (CISO)?** - Do they sit on the board? **At what committee(s), if any, is cyber security discussed?**	*This section explores the role of the board and committees in their cyber security management.*

Participants may reference audit, cyber or none. ASK ALL WHO HAVE A COMMITTEE: ● 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?	
4. Designated responsibility/oversight	**5-6 minutes**
The next few questions will be about how your board engages with cyber security. (Refer to survey answers Q_BOARDGOVERN) (If answered a1) **In the survey you said that one or more board members' roles included oversight of cyber security risks.** ● What does this role entail? ● Do board members understand your organisation's cyber security defences, and key cyber security threats? ● Do they have adequate access to cyber security expertise? ● 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)?	*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.* *Please ask all questions that are relevant, for example, if the participant answered a1 and b1 ask **the first 3** questions. If neither a1 nor b1 is yes, ask the final question.*

(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.** ● 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? (If answered a1 *and* b1) **How effectively do the designated staff member and board member(s) responsible for cyber security work together, if at all? What works well/not so well?** ● How do they share information with each other? / How frequently? ● What information do they usually discuss? PROBE ON: - Cyber KPIs (key performance indicators) - Cyber news - Cyber projects/investment - Cyber risks in the business - Cyber threats/attacks ● Do they generally discuss internal or external cyber threats? (If neither a1 nor b1 is yes) **In the survey you indicated you were not aware that a specific board member has oversight of cyber security risks, or that a designated staff member reports to the board on cyber security issues.** ● Who in the organisational structure would have responsibility for cyber security issues and risks? ● Does the board receive updates on cyber security issues? IF YES: Who	

provides these updates? How often? ● What are the advantages and disadvantages of these arrangements? PROBE. ● Are there any plans to change these arrangements in future? IF YES: What changes are likely? When might these changes be implemented? Are there any barriers?	
5. Supply chains and external consultants	**7-9 minutes**
I would now like to talk a bit about supply chains. **Is cyber security considered as a risk when you choose a supplier? How does it influence/factor into your choices?** ● **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: - Impact of legal protection - Greater knowledge/awareness ● **What are the reasons behind investing in your supply chain risk management? (PROBE ON whether investment had been influenced directly or indirectly by experiences of cyber security incidents)** - **Has your priority of investing in supply chain risk**	*This section explores how organisations manage the cyber security risks of their supply chain.*

management changed over time? IF YES: Why? ● Does your organisation have a strategy in place to address cyber security threats that emerge from your supply chains? PROBE ON: - Whether this strategy sets out the acceptable level of risk that your organisation can tolerate ● IF ORGANISATION IS CYBER ESSENTIALS CERTIFIED: Does your organisation use Cyber Essentials as a tool to manage threats that emerge from your suppliers? *IF YES, PROBE ON:* - *Why do you use CE to manage supply chain risks?* - *Does it save time and money?* - *Do they make it mandatory for suppliers to get CE certified, or do they recommend it?* ● 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? **Does your organisation currently use external IT or cyber security consultants?** IF NO:	

● Probe to understand why not – lack of trust, too expensive etc. IF YES: ● Why did you decide to use external consultants? ● What do these consultants do? ● How did you choose the consultant? ● What factors did you consider when making this choice? ● How much, if at all, would you say you trust these external consultants?	
6. Corporate/external reporting	**4-5 minutes**
Earlier we talked about your internal reporting processes. In the final couple of minutes, I would like to talk about your annual reporting. In your most recent annual report, what kind of things did you include about your cyber security? *PROBE ON*: ● **What governance processes are in place for managing cyber resilience?** ● **How the organisation assesses its cyber resilience** ● **Type of cyber risk strategy** - How often the strategy is reviewed - Whether you receive independent assurance of the strategy	*This explores the type of information that organisations include in their reports on cyber security.*

- Prompt to confirm if it is clear in the strategy what is an acceptable level of risk for the organisation to take on. ● **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? **Why do you choose to include these things as opposed to others?** *(could give example of those not mentioned)* IF EXPERIENCED A BREACH OR CRIME: **Finally, have you ever reported a cyber breach or cyber crime?** *IF YES, PROBE ON:* - Why did you decide to report this? - Where did you report it to? - How was your experience of reporting it *IF NO, PROBE ON:* - Why did you decide not to report this?	
Overall, what do you think I should take away from the discussion today? Is there anything you feel that we haven't covered today that you would like to share? Inform about next steps and incentive. THANK AND CLOSE	*Wrap up the interview*

Appendix C: Further information

The Department for Science, Innovation and Technology 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
- Benjamin Swannell, Ipsos
- Finlay Procter, Ipsos
- Jayesh Navin Shah, Ipsos
- Scott Nisbet, Ipsos
- Karl Ashworth, Ipsos

The responsible DSIT analyst and statistician for this release is Emma Johns (cybersurveys@dsit.gov.uk).

For general enquiries contact:

Department for Science, Innovation and Technology
100 Parliament Street
London
SW1A 2BQ

Telephone: 020 7211 6000

DSIT statisticians can be followed on X (formerly known as Twitter) via @DSITInsight.

This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos Terms and Conditions which can be found at https://www.ipsos.com/sites/default/files/ipsos-terms-and-conditions-uk.pdf.