Department for Science, Innovation and Technology	
Cyber Security Longitudinal Survey Wave Five: Technical Annex	

Fieldwork monitoring Cyber Security Longitudinal Survey Wave Five

Technical Annex

This Technical Annex provides details of the methodology of the Cyber Security Longitudinal Survey (CSLS) Wave Five. It covers the quantitative survey (fieldwork June – August 2025) and qualitative element (carried out in August – September 2025), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

This annex supplements a main Analytical Release 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 organisations change and improve over time.

It also examines how organisations' cyber security actions relate to the likelihood and impact of a cyber incident.

This is the fifth research year, and therefore the main objective of this report is to establish any significant trends that have occurred across the four years of the research. The quantitative survey was carried out in June – August 2025 and the qualitative element in August – September 2025.

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 Five pertains to the fifth year of a longitudinal research project.

For this study, we undertook a random probability multimode (telephone and online) survey of 521 UK businesses and 273 UK registered charities. The main stage survey took place between 2 June - 25 August 2025. The data for businesses and charities have been weighted to be statistically representative of these two populations. Please note that the cross-sectional and longitudinal analysis has been weighted differently, which is detailed in section 2.6 of this technical report.

In addition, we carried out 24 in-depth interviews in August and September 2025 to gain further qualitative insights from some of the organisations that answered the survey.

The CSLS is designed to permit both cross-sectional and longitudinal analysis of medium and large-sized businesses and high-income charities (see below). Where possible, the study utilised repeat observations with the same organisations and supplemented any dropouts from the survey with a fresh sample cohort in each year. This approach allows for better cross-sectional analysis, as it ensures a representative sample overall for each survey wave. This approach also adds flexibility to the longitudinal design as there is no hard requirement for organisations to take part in all waves.

The longitudinal nature of the Wave Five survey means that 70% of the sample interviewed were the same organisations from Wave Four (i.e. are part of the 'panel' sample). A top-up or 'fresh' sample was also used 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). 30% of Wave Five sample interviewed were fresh sample to account for attrition or dropout.

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, and cyber insurance
- 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 one business in Wave Five.

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 2025 (CSBS), which is an annual study of UK businesses, charities and education institutions.

This study differs from the CSBS in several important respects:

- it uses a longitudinal design to better identify drivers for change in cyber security and cyber resilience 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), charities of all incomes 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

There are a number of questions which are surveyed in both the CSBS and CSLS. This is to account for the analysis implemented, such as longitudinal data in CSLS. For cross-sectional analysis of all business and charity sizes, overlapping questions should be taken from CSBS data. These 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_REASONFORNOINSURANCE	Asked to those who currently do not have a insurance against cyber security Is there a reason why you do not have cyber insurance? Is it…?
Q_RULES	And which of the following rules or controls, if any, do you have in place?
Q_COMPLY	Which of the following standards or accreditations, if any, does your organisation adhere to?
Q_INCIDENT	Have any of the following happened to your organisation in the last 12 months? The change in this question refers to the text change to the answer codes to better align with CSBS
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?

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)
- 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 between Wave Four and Wave Five was 46%, meaning that almost half of the panel that agreed to be recontacted did not complete the survey at Wave Five. The comparison across waves becomes more risky when the base per question drops below 30 respondents.
- 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.

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

Ipsos developed the questionnaire and all other survey instruments with guidance and input from DSIT, who also gave final approval of the questionnaire. The Wave Five questionnaire was largely based on the Wave Four version, with only one new question included in the survey.

Waves One, Two and Four all included pilot testing of fieldwork (a three day pilot). This was deemed unnecessary in Wave Three due to the minimal changes to the questionnaire.

Cognitive testing was implemented in Wave One to ensure data accuracy and question comprehension. While Waves Two, Three and Four did not explicitly cognitive test questions, the pilot stages allowed for analysis of comprehension and data.

Since the Wave Five questionnaire was largely unchanged, with only one additional question, Ipsos and DSIT determined that cognitive testing was unnecessary. However, a pilot was conducted from 2 - 6 June 2025 as part of the fieldwork.

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 changes between Waves Two and 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.

Questionnaire changes for Wave Four were made to reflect developments in DSIT priorities. This means that while comparability with Waves One, Two and Three has been maintained across core questions, some additional questions were added to explore potential long term changes in, and impacts of, organisations’ cyber security experiences and actions in greater depth. There were seven new questions added for Wave Four, listed below:

- **Q_REASONFORNOINSURANCE**. This was added to Wave Four to understand the reasons why organisations who didn’t have cyber security insurance didn’t have a policy in place

- **Q_CYBERSECURITYBUDGET.** This was added to Wave Four to understand how cyber security budgeting has changed over time
- **Q_BUDGETCHARACTERISTIC.** This was added to Wave Four to understand the characteristics of organisations' cyber security budget
- **Q_ATTITUDETOWARDSCYBERSECBUDGET.** This was added to Wave Four to understand organisations attitude towards their cyber security budget
- **Q_REASONFORNOINSURANCE.** This was added to Wave Four to understand why organisations do not have a cyber security insurance policy
- **Q_DRIVINGCHANGE.** This was added to Wave Four to understand what factors drive organisations to change their cyber security attitude
- **Q_PANELRECON2.** A key element of a longitudinal survey is to ensure that the same organisations are interviewed each year. This question aims to re-iterate the value of becoming part of the panel sample of organisations

The questions removed in Wave Four are listed below. These were removed to ensure that the length of interview did not take longer than required.

- **Q_CHARITYINCOME.** In the last financial year, was the annual income of your charity…?
- **Q_VPN.** This has been merged with **Q_RULES**
- **Q_AIML** Does your organisation deploy any cyber security tools that use AI or machine learning?
- **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_STATEMENT.** Did you include anything about cyber security in your organisation's most recent annual report?
- **Q_PEER.** In the last 12 months, have you ever reviewed or changed any cyber security policies or processes as a result of the following? This has been merged with **Q_INFLUENCE**
- **Q_BOARDTRAIN.** This has been merged with **Q_BOARDTRAINFREQ**
- **Q_FREQ.** Approximately, how often in the last 12 months did you experience any of the cyber security incidents you mentioned? Was it…?
- **Q_RANSOM.** In the case of ransomware attacks, does your organisation make it a rule or policy to not pay ransomware payments?
- **Q_DISRUPT.** What kind of incident was this?
- **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…?
- **Q_DAMAGEDIRS/Q_DAMAGEDIRSB.** 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.
    - Was it approximately…?
- **Q_DAMAGEDIRL/Q_DAMAGEDIRLB.** 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.

Was it approximately…?

- **Q_DAMAGESTAFF/Q_DAMAGESTAFFB.** 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. Was it approximately…?
- **Q_DAMAGEIND/Q_DAMAGEINDB.** 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

  Was it approximately…?
- **Q_COSTA/Q_COSTB.** 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? Was it approximately…?

Questionnaire changes between Waves Four and Five of the survey was limited to the amendment of pre-existing questions, for maximum comparability between waves of the survey. The amendments and one addition made were:

- **Q_GUIDANCE_v3.** This was updated in Wave Five, replacing Q_GUIDANCE_v2 from Wave Four to present a focused set of governance-level guidance

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 (for example to organisations that wanted more information) also included a link to the GOV.UK page.

2.3 Sampling

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

Panel sample

Wave Five of the CSLS included repeat observations with the same organisations that had been interviewed in Wave Four of the survey. This is the same as the first four waves of the CSLS.

After those who had not given permission to be re-contacted for Wave Five had been excluded, there were 1,046 cases within the panel sample, comprised of 574 businesses and 472 charities. A breakdown of the 574 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	0	1	2
C	Manufacturing	60	15	12	87
F	Construction	20	2	8	30
G	Retail or wholesale (including vehicle sales and repairs)	46	15	14	75
H	Transport or storage	22	5	5	32
I	Food or hospitality	19	7	8	34
J	Information or communication	38	8	2	48
K	Finance or insurance	15	4	5	24
L	Real estate	5	1	1	7
M	Professional, scientific, or technical	45	9	7	61
N	Administration	48	7	21	76
P	Education (excluding public sector schools, colleges, and universities)	7	1	4	12
Q	Health, social care, or social work (excluding NHS)	51	5	10	66
R	Arts or recreation	11	2	2	15
S	Other service activities	2	1	2	5
Total		390	82	102	574

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

Table 2.2 Panel attrition across all five waves

	Wave 1	**Wave 2**	**Wave 3**	**Wave 4**	**Wave 5**
Total completed interviews	1741	1061	852	1222	794
Panel interviews	-	674	451	321	556
Cross sectional interviews	1741	387	401	901	238
Agree to be in panel sample	1405	899	724	1046	698
Retention rate	81%	85%	85%	86%	88%
Attrition rate	19%	15%	15%	14%	12%

A total of 3,668 organisations have taken part in the survey across all five waves, including both cross-sectional and panel completes.

Top-up sample

To address attrition 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 Wave 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 37,800 according to the latest Business Population Estimates).
- large businesses with 250+ staff (a population of 8,250 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. Unlike Waves One to Wave Three, the sample frame for businesses for Wave Four and Five was sourced from Market Location business sample. Wave Five also included fresh sample improvement and enhancement via Sample Solutions. As this sample provider operates independently of Market Location, fresh sample without email addresses were attributed from Sample Solution's unique database.

Exclusions from the Market Location 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 Five.

[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.

Charity population and sample frames (including limitations)

The target population of charities is high-income charities with £1 million or more in annual income (a population of 9,288 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. Ipsos, at DSIT's request, 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.

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

Most of the charity sample was achieved via panel sample, so only 109 fresh charity leads were added for Wave Five.

Business sample selection

In total, 7,494 'fresh' businesses were selected from the latest available version of Market Location for the survey.[2]

We determined this to be an accurate business sample based on the current panel needs, along with Waves One, Two and Three of the CSLS. The principal challenge considered was to mitigate against the risk of varying sample quality experienced in similar surveys in recent years (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 the majority of large

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

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 businesses was boosted relative to medium businesses.

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 (SIC K)
- information and communications (SIC J)

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

Charity sample selection

The charity sample was treated as a recontact sample, drawn from organisations that completed the Wave 4 survey. This approach supports the longitudinal design of the study by enabling comparisons over time within the same organisations. It also improves efficiency by reducing the need for fresh sampling and helps maintain consistency in respondent understanding of the survey content.

Alongside increasing the business sample, Ipsos also expanded the charity sample. However, the majority of completed charity interviews came from the panel (97%), with only the remaining 3% (9 interviews) needed to meet the targets.

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 Ipsos' 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 Four participants that did not give consent to be re-contacted for Wave Five

Where Market Location fresh business sample did not have a name or email address, this was enhanced by Sample Solutions to reduce any risks on response rate.

Table 2.3 breaks down the usable fresh business sample by size and sector, a total of 7,494 fresh business leads remained post-cleaning.

Table 2.3 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	23	76	79	178
C	Manufacturing	201	346	170	717
F	Construction	49	110	69	228
G	Retail or wholesale (including vehicle sales and repairs)	248	392	308	948
H	Transport or storage	73	198	156	427
I	Food or hospitality	147	149	107	403
J	Information or communication	286	268	180	734
K	Finance or insurance	371	336	328	1035
L	Real estate	27	54	53	134
M	Professional, scientific, or technical	231	405	268	904
N	Administration	193	314	309	816
P	Education (excluding public sector schools, colleges, and universities)	13	50	39	102
Q	Health, social care, or social work (excluding NHS)	222	183	173	578
R	Arts or recreation	43	75	61	179
S	Other service activities	21	55	35	111
Total		2148	3011	2335	7494

Sample batches

For businesses and charities, the usable sample for the main stage survey was randomly allocated into separate batches. There was a total of four batches released in two stages. Each stage had an email send out and a batch released to the Telephone team.

The first batch was for the Pilot which included 335 leads shared with the telephone team and emailed. 62 panel leads were then called and emailed to finish the pilot period. The email batch were sent two reminders before they were released to the telephone team to be dialled.

Batch two was the first batch post the pilot and included 7,516 leads that were sent to the telephone team and all leads with an email address were emailed first before being released to the telephone team.

Batch three included 627 leads that were released to the telephone team, after those with email addresses were emailed first before being released to the telephone team.

Across all sample groups, three batches of sample were released throughout fieldwork. We aimed to maximise the response rate by 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 85,410 leads were released.

2.4 Fieldwork

Ipsos carried out fieldwork between 2 June - 29 August 2025 using a Computer-Assisted Telephone Interviewing (CATI) option and an online survey option.

In total we completed 794 interviews with:

- 521 businesses
- 273 charities

The average interview length was c.25 minutes for all groups.

70% of the interviews were with repeat organisations from previous waves of the survey.

- 556 were from the panel sample (292 businesses, 264 charities)
- 238 were from the fresh sample (229 businesses, 9 charities)

Fieldwork preparation

Prior to fieldwork, the Ipsos research team briefed the telephone interviewing team in a video call. Interviewers 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.

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
- 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 and instructions should they wish to complete the survey online. These were sent to both specific individual email addresses as well as generic email addresses.
- 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 the Institute of Chartered Accountants in England and Wales (ICAEW), Tech UK and the ABI, 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

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.

- 611 interviews (77%) were completed through the CATI option
- 183 interviews (23%) 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% 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 2.4 shows the final outcomes and the adjusted response rate calculations for businesses and charities.

Table 2.4: 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	7,494	109	574	472
Completed interviews	229	9	292	264
Incomplete interviews	1,213	83	11	41
Unusable leads	4,239	124	60	119
Refusals [3]	1,167	64	11	45

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

556 out of 1,046 panel leads from Wave Four, or 53% took part in Wave Five again, including 56% of charities and 51% of businesses, which was in line with expectations.

1 The adjusted fresh sample response rates[4] for Wave Five were 9% for businesses and 29% for charities. The business fresh sample response rate is broadly similar to the overall response rates observed in CSBS 2024 (7% for businesses), and in line with CSLS Wave Four (10%). The charity fresh response rate is based on a very small sample size, so should not be compared with other fresh charity response rates.

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

- 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

Similar to previous waves, Wave Five length of interview remains at c.25 minutes. The increase in the survey length from c.22 minutes in the first wave of the survey, to c.25 minutes in Waves Two, Three, Four and Five remains an issue impacting response rate – interviewers must

[3] 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.

[4] 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.

mention the average length to respondents when they introduce the survey, and respondents are naturally less inclined to take part in longer interviews.

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.[5] 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 and others are added. 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

Coding

We did not undertake SIC coding. Instead, the SIC 2007 codes that were already in the Market Location 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.

Cross-sectional 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 fewer 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 to 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 DBT Population Estimates 2024.

[5] 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).

Consistent with Waves One, Two, Three and Four, 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 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 were applied separately to the unweighted cross-sectional data from all waves, outline in section 5.4 of this technical report.

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

Table 2.5: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %[6]
Size		
Medium (50–249 staff)	60.1%[7]	81.6%
Large (250-499 staff)	18%	9.2%
Very large (500+ staff)	21.7%	8.8%
SIC / Sector		
B/D/E: Utilities or production	1%	1.3%
C: Manufacturing	13.6%	15.9%
F: Construction	5.4%	5.2%
G: Retail or wholesale (including vehicle sales and repairs)	14.8%	14%
H: Transport or storage	5.6%	4.4%
I: Food or hospitality	4.8%	8.8%
J: Information or communication	8.8%	6.5%
K: Finance or insurance	3.6%	3.3%
M: Professional, scientific, or technical	11.5%	10.9%
N/L: Administration or real estate	12.5%	13.6%
P: Education (excluding public sector schools, colleges, and universities)	1.9%	1.9%
Q: Health, social care, or social work (excluding NHS)	12.1%	10.7%
R/S: Entertainment, service or membership organisations	4.4%	3.5%

2.7 SPSS data uploaded to UK Data Archive

Derived variables

In Wave Five, derived variables remain in the SPSS file. All the derived variables are nets for answer codes for each question. These derived codes are:

- Bgovern3 – any board member that has oversight of cyber security risks
- Ident5 – did any action to identify cyber security risks
- Ident6 – did all four action to identify cyber security risks
- complyx7 – comply to any standards or accreditations
- Incident12 – this has 2 derived answer codes, one to identify organisations that had any incident in the past 12 months and one to identify if an organisation had no incidents

[6] 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

[7] Includes 17 interviews with panel businesses that had 50-249 employees when first interviewed, but fewer than 50 employees in 2025 - these were therefore still considered eligible.

- Incident13 – this has 2 derived answer codes, one to identify organisations that had any incident, excluding phishing in the past 12 months and one to identify if an organisation had no incidents
- Rule10 – organisations that had all five cyber essentials technical controls
- Rule11 – organisations that had any of the five Cyber Essentials technical controls
- Gov6 – this has 2 derived answer codes, one to identify organisations that have any of the five documents in place to help manage cyber security risks and one to identify organisations that have none of the documents in place to help manage cyber security risks
- Gov7– this has 2 derived answer codes, one to identify organisations that have all five documents in place to help manage cyber security risks and one to identify organisations who don't have all five documents in place to help manage cyber security risks
- qsizex1 – is a variable that combines business size for organisations with 250+ employees
- qsizex2 – is a variable that combines business size for organisations with 500+ employees
- sectorx1 – is the variables that nets the SIC codes for Admin/real estate and Entertainment, service or membership organisations
- bus_reg3 – is the variable that has the business regions for the 4 nations
- secbudgetx – is the variable for cyber security budget increase or decrease
- budgetcharx – is the variable for whether budget is sufficient or insufficient

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.[8] 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.

[8] 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 24 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 to 60-minute interview on the same topic. In total, 23 respondents (96%), including 15 businesses (94%) and 8 charities (100%), 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.

We carried out interviews with 16 businesses and 8 charities.

3.2 Recruitment quotas and screening

We carried out recruitment for the qualitative element by email and telephone using a specialist business recruiter. We offered a shopping voucher or charity donation of £70 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 income bands for charities.

Fieldwork

The Ipsos research team carried out all fieldwork in August and September 2025. We conducted the 24 in-depth interviews through a mix of telephone and Microsoft Teams. Interviews lasted around 45 to 60 minutes on average.

The qualitative phase was informed by a behavioural science approach, which provides a structured way of understanding the mechanisms underpinning behaviour and subsequently what needs to be changed to facilitate desired behaviours and more optimal decision making. With the aim of facilitating optimal engagement with cyber security practices, processes and policies, we used the COM-B framework to identify the influences of behaviours to engage.

COM-B is comprised of three components:

- Capability: having physical and psychological skills, strength and stamina, and the knowledge, to engage in necessary mental processes for a behaviour to occur
- Opportunity: the opportunity afforded by the environment, involving time, resources, locations, cues, and physical ease; and the opportunity afforded by interpersonal influences, social cues and cultural norms that influence the way we think about things
- Motivation: how we think – including plans (self-conscious intentions) and evaluation (beliefs about what is good or bad); and automatic processes involving emotional reactions, desires (wants and needs), impulses, inhibitions, drive states and automatic responses.

Ipsos and DSIT worked together on the topic guide with the final topic guide being reviewed and approved by DSIT.

The guide covered the following broad questions:

- Business / charity background as well as respondent background
- Business / charity capability concerning cyber security – resource and expertise, role of senior leadership, approach to cyber risk and perceived strengths and weaknesses of cyber security capabilities
- Business / charity opportunity concerning cyber security – resource and support available, best practices or guidelines followed, opportunities and barriers to improving cyber security and support needs
- Business / charity motivation concerning cyber security – importance of cyber security, drivers to improve attitudes, competing priorities, challenges or barriers and how cyber security compares to other risks
- Direct experience of cyber security incidents including its effects and impacts.
- The role of external information including its effects and impacts
- The role of requirements and advice including its effects and impacts
- The role of other factors such recent information from customers, clients, partners, suppliers, government or other stakeholders received related to cyber security including its effects and impacts
- Assessing the overall impact of specific actions taken that were identified throughout the interview including its impact on attitudes towards cyber security

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

Tables 3.1 and 3.2 show a profile of the 16 interviewed businesses by size and sector.

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

SIC 2007 letter	Sector description	Total
C	Manufacturing	2
F	Construction	2
G	Retail or wholesale (including vehicles)	2
H	Transport and storage	1
J	Information or communication	2
K	Finance or insurance	2
L	Real estate	1
M	Professional, scientific or technical	1
Q	Human health and social work activities	2
S	Other service activities	1
	Total	**16**

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

Size band	Total
Medium (50-249 staff)	10
Large (250-499 staff)	6
Total	**16**

3.2 Analysis

Throughout fieldwork, the core research and fieldwork team discussed findings as they emerged. We held one analysis meeting over MS Teams with the core research and fieldwork team at the end of fieldwork. In this session, the team discussed the findings from individual interviews, and we drew out key themes, recurring findings, and other patterns across the interviews.

We also recorded all interviews and summarised them in an Excel analysis framework, 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 **794 completes** and the average (mean) survey length was **25 minutes**. Therefore, the research compliance cost for the quantitative survey this year was [794 × 25 minutes = **330 hours**]
- the qualitative research had **24 respondents** and the average interview length was around **50 minutes to 60 minutes**. Respondents completed the qualitative interviews in addition to the quantitative survey. The research compliance cost for the qualitative strand this year was a maximum [24 × 60 minutes = **24 hours**]

In total, the compliance cost for the CSLS Wave Five was **354 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 where requested

Chapter 5: Longitudinal analysis

5.1 Overview

The cross-sectional analysis shows aggregate trends in cyber experiences and protective behaviours. However, these trends hide important patterns of change. Organisations do not follow predictable paths. An organisation experiencing a cyber incident one year may not face one the next year. Similarly, protective activities (like cyber security audits) may start and stop from year to year.

The level of activity in any given year comes from three groups:

1. Organisations who undertook the activity last year and continue this year.
2. Organisations who did not undertake the activity last year but started this year, which we call positive change.
3. Organisations who undertook the activity last year but stopped this year, which we call negative change.

Additional changes may occur that are not fully captured here. For example, organisations might change the number of activities they do, or replace one activity with an equivalent or upgrade, such as moving between ISO accreditation and Cyber Essentials.

Longitudinal data allows us to track specific activities over time. For standards adherence, we can see the average proportion of organisations adhering to standards at different time points, how many organisations move from non-adherence to adherence, and how many move from adherence to non-adherence. This reveals the rates of positive and negative change underlying the aggregate trends.

The longitudinal panel measures any changes across two time points, creating a two-time panel. Time point 1 relates to the first time a longitudinal respondent provided data, and time point 2 relates to the second point in time they responded.

Throughout this report, we use a change ratio to measure the relationship between positive and negative change. A ratio of 1 means that positive and negative change cancel each other out. A ratio greater than 1 shows that positive change exceeds negative change. A ratio less than 1 indicates that negative change exceeds positive change. This ratio helps us compare behaviour change between different types of organisations.

We examine two main organisational types. The first distinguishes between charities, medium-sized businesses with 50-249 employees, and larger businesses with 250 or more employees. The second type is defined by cyber incident experience in the last 12 months prior to interview. This includes organisations with no incident, those with an incident but no impact or outcome, and those with an incident that produced an impact and/or outcome.

Based on organisational characteristics, we anticipate certain patterns. However, there are instances where the cross-sectional trend appears relatively flat but suddenly shows a sharp growth spike. For example, investment in threat intelligence suddenly spikes at Wave 5, yet the longitudinal data shows the negative change rate exceeding the positive change rate. A longitudinal panel study collects data from the same group of participants at multiple time points, called waves. In this study, the information covers Waves 1 through 5. Approximately 28% of the participants joined in Wave 4, and their data is part of the analysis for Wave 5. In Wave 5, there was a noticeable increase in activity when viewed alone. However, when you

look at the longitudinal data which combines all waves, this spike is less apparent due to the influence of data from Waves 1 through 4. Therefore, the overall trend over time appears more steady, and sudden changes between waves, such as those between Waves 4 and 5, are less visible in this type of analysis. It is also apparent that for this particular activity, the proportion answering "Don't Know" decreases over time, which adds further complexity to the patterns of change between waves. The two-time panel is therefore best placed to understand general change between two consecutive years across the observation period and should not be used to try to explain any sudden change solely limited to two consecutive years.

The outcomes chosen for analysis represent a selection of activities, policies, procedures and behaviours that help promote cyber resilience. These are shown in Section 5.2. Additionally, experience of cyber incidents serves both as an outcome and as a breakdown variable. It is of interest as an outcome to help understand the extent to which organisations are subject to consistent incidents or no incidents. Cyber incidents are classified as none, an incident with no adverse consequences, or an incident with adverse consequences. Consequently, cyber incident experience is also used as an organisational breakdown variable to assess the extent to which positive and negative change are influenced by the adversity of the cyber experience.

Given the relatively small longitudinal sample size, Section 5.3 outlines how we made best use of the dataset to analyse stability and change over two time points, while preserving sufficient sample sizes to enable breakdowns by organisational characteristics. However, this approach does limit the number of waves over which an organisation's experience can be tracked. Looking ahead, potential future waves could provide the first opportunity to explore change across three time points, allowing for more robust insights into the progression of cyber resilience and related behaviours over time.

5.2 Variables included in the analysis

Candidate variables were selected for analysis based on initial discussions between DSIT and the research team and were then further refined after inspection of initial raw frequencies. The candidate variables were selected based on considerations of policy relevance in terms of policies, procedures and behaviour relating to improving cyber resilience. The candidate list was further refined by ensuring the numbers in the tables were of sufficient size to produce robust statistics. Additionally, a measure of cyber incident experience was created from the derived variables identifying any experience of a cyber incident and any overlap between an incident with an impact or outcome arising from the incident. These were assumed to reflect increasing levels of adverse experience, respectively. This variable was used both as an outcome and the first interview classification was also used as a breakdown variable to explore change over time in other outcome measures. Additionally, organisations were grouped as follows: medium businesses (50-249 employees); large businesses (250+ employees); and charities. This variable was also used as a breakdown characteristic for changes in other outcomes over time.

Table 5.1: Questions included in the analysis

Question Code	Question text
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_GOV	Does organisation have documentation in place to help manage cyber security risks?
Q_INCIDMAN	Do you have any written processes for how to manage a cyber security incident, for example, an incident response plan?
Q_SUPPLYHOW	Which have you done with any of your suppliers/suppliers or partners in the last 12 months?
Q_SUPPLYRISK	In the last 12 months, has your organisation carried out any work to formally assess/manage potential cyber security risks presented by any suppliers/partners?
Q_INSUREX	Which of the following best describes your situation?
Q_BOARDGOVERN	Does your organisation have... One or more board members whose roles include oversight of cyber security risks/ A designated staff member responsible for cyber security, who reports directly to the board?
Q_BOARDDISCUSS	Over the last 12 months, roughly how often, if at all, has your board discussed or received updates on your organisation's cyber security?
Q_BOARDENGAGE	How much would you agree or disagree with... The board integrates cyber risk considerations into wider business areas?
Q_BOARDTRAINFREQ	On average, how often does the board receive cyber security training?

5.3 Constructing the longitudinal dataset

As described above, the CSLS methodology was designed such that it includes both an annual top-up of new organisations (businesses and charities) to the sample in each year and further interviews of organisations previously interviewed in the earlier years. Currently, in Wave Five the sample comprises cohorts with their first interview, along with cohorts who had their first interviews at Waves Two, Three, Four and Five. For a longitudinal analysis, it is imperative that each cohort responds to at least a second interview.

The structure of the longitudinal data set was initially as a 'long' file, meaning each unique respondent had as many rows in the dataset as they had interviews. For analytical convenience, this dataset was reshaped into a 'wide' dataset, with each respondent having a single row in the dataset. Multiple occurrences of the same variable at each interview were stored in separate columns denoted by a suffix of "_1" for the first interview, "_2" for the second interview and so on. The 'long' dataset comprised 5,670 rows, representing 3,668 respondents. Table 5.2 demonstrates the patterns of response seen across the five survey waves. Response Pattern 1 shows there were 238 cases in the dataset contributing nothing to the longitudinal dataset because their first interview took place at Wave 5 and they have not yet had the chance to be included for a second interview. Response Pattern 2 shows Wave 4 starters who responded to their first interview at Wave 4 but dropped out of the study after this. Response Pattern 3 shows Wave 4 started with a follow-up second interview at Wave 5. Excluding the 238

Wave 5 starters, gives a total of 3,430 longitudinal cases, with 1,292 responding for a second interview and 2,138 dropping out after their first interview.

Table 5.2: Longitudinal response patterns

Response pattern	Wave 1	Wave 2	Wave 3	Wave 4	Wave 5	N
1	0	0	0	0	1	238
2	0	0	0	1	0	537
3	0	0	0	1	1	364
4	0	0	1	0	0	282
5	0	0	1	1	0	62
6	0	0	1	1	1	57
7	0	1	0	0	0	252
8	0	1	1	0	0	76
9	0	1	1	1	0	20
10	0	1	1	1	1	39
11	1	0	0	0	0	1067
12	1	1	0	0	0	358
13	1	1	1	0	0	173
14	1	1	1	1	0	47
15	1	1	1	1	1	96
Total						3668

The design of the survey does not allow for straightforward separate analysis of each cohort of longitudinal respondents individually. For example, only 96 cases responded to all five waves from the first cohort and this number is both too small to produce robust breakdown statistics and would likely need substantial weighting readjustment to become representative. A more efficient approach was to combine the first four cohorts into a single dataset taking only their first two interviews. The structure of this "two-period" panel is shown in Table .3 Thus, the 674 Wave 1 starters contribute their data from the first (Wave 1) and second (Wave 2) interviews. The 135 cases from the second cohort starting at Wave 2 contribute their first interview (Wave 2) and their second interview (Wave 3), and so on. Consequently, a 'wide' dataset comprising 1,292 respondents has data stored from the first interview in columns identified with a "_1" suffix, whereas their corresponding second interview data are stored in separate columns and identified by the "_2" suffix.

Table 5.3: Design of the two-period analytic panel

Cohort	Time 1	Time 2	N
1	Wave 1	Wave 2	674
2	Wave 2	Wave 3	135

3	Wave 3	Wave 4	119
4	Wave 4	Wave 5	364

This approach enables maximum use of the longitudinal responses in that it increases the size of the dataset permitting a more detailed breakdown of longitudinal response patterns. However, a drawback of this approach arises from uneven sample sizes starting their first interview across the first four waves of the study. The extent of change between Wave 1 and Wave 2 predominates the general analysis of comparisons between the first and second interview because 674 (52%) of the 1,292 longitudinal two-period panel started at Wave 1 of the study (see Table 5.3). Consequently, any changes between 2022 (Wave 2) and 2023 (Wave 3) are only represented by 135 (10%) cases, which can dampen any change appearing between 2022 and 2023 in the analysis undertaken here.

A key research objective for this report was to explore the relative rate of change to a positive behaviour from not undertaking it at Time 1 but taking it up at Time 2 relative to the rate of active at Time 1 but not at Time 2. The larger sample size provided by this approach makes it possible to produce robust estimates of change from a negative state to positive state between the first and the second interview. Similarly, the number of changes from negative to positive can also be identified. These two positive and negative change rates can be compared to assess the extent to which the rate of positive change exceeded negative change, or vice-versa. These positive, negative and relative rates were then broken down by cyber security incident experience and by organisational type/size. However, even this approach does not provide a sufficient sample size for a robust 4-way breakdown of cyber attack experience at Time 1 and Time 2 by positive and negative change rates. Consequently, it has been necessary to compare change rates only by their Time 1 cyber attack experience and not by their combined Time 1 and Time 2 cyber experience.

5.4 Weighting for survey attrition

Non-response to the survey can result in estimates that are over-reflective of characteristics of those organisations that remain at the expense of those that have left the survey. To help counter this, respondents at their second interview were readjusted to reflect the set of respondents to the first interview for each cohort. The dataset for analysis was those organisations that had completed a first interview and were therefore eligible for a second interview (n = 3,430). A variable with the binary of response = 0 (n = 1,292) versus attrition = 1 (n = 2,138) was created for the 3,430 longitudinal cases and an initial set of cross-tabulations was undertaken comparing attrition rates between categories of several variables of key interest (Table 5.1 shows the list of variables included in the analysis).

A binary logistic regression model used the binary attrition variable as the outcome and a selection of predictor variables identified from the cross-tabulations. These were:

- Wave of entry to the survey
- Organisation type/business size
- Time 1 cyber incident experience
- Designated staff member reporting cyber security issues to board
- Business Continuity Plan to cover cyber security
- Adherence to Cyber Essentials Standards

Table 5.4: Attrition model coefficients

Variable	Estimate	Std. Error	t value	P
Intercept	0.580	0.103	5.604	0.000
Started Wave 2	0.143	0.131	1.092	0.275
Started Wave 3	0.373	0.133	2.811	***0.005***
Started Wave 4	-0.001	0.089	-0.007	0.995
Business 250+ employees	0.195	0.101	1.941	0.052
Charity	-0.220	0.082	-2.664	***0.008***
Cyber experience: incident only	-0.148	0.100	-1.490	0.136
Cyber experience: incident with impact and/or outcome	-0.235	0.100	-2.344	***0.019***
No: Designated staff member reporting cyber security issues to board	0.047	0.082	0.577	0.564
DK: Designated staff member reporting cyber security issues to board	0.539	0.236	2.284	***0.022***
Yes: Adherence to Cyber Essentials Standards	-0.280	0.099	-2.836	***0.005***
No: Business Continuity Plan to cover cyber security	0.114	0.098	1.163	0.245
DK: Business Continuity Plan to cover cyber security	0.482	0.146	3.302	***0.001***

Note: The 'intercept' subsumes the effect for the reference group, which includes organisations: that started at Wave 1, businesses with 50-249 employees, has a designated staff member reporting cyber security issues to the board, no adherence to Cyber Essentials Standards, has a Business Continuity Plan to cover cyber security.

The inverse of the probability of attrition was calculated using the model coefficients, which was used as the Time 2 attrition weight. This weight was multiplied by the initial cross-sectional weight to produce a Time 2 longitudinal weight. The properties of the weights are summarised below in Table 5.5.

Table 5.5: Properties of the weights

Value	Initial	Non-response	Longitudinal
Min	0.24	1.86	0.73
5%	0.35	2.02	1.32
50%	1	2.54	2.38
95%	1.39	3.72	4.13
Max	3.79	5.96	9.67

Sum	1,284	3,416	3,362

Note: based on the 1,292 longitudinal respondents over their first two interviews

Table 5.5 shows the development of the three weights for the two-time panel of the 1,292 'cases included in the longitudinal analysis. The initial weight was inherited from the cross-sectional weight at the first interview. The sum of the initial weights was 1,284 and therefore just under the 1,292 cases included in the dataset. This initial weight was the starting point for the attrition and non-response weights. Correspondingly, the attrition (non-responses) and longitudinal weights also sum to just under the 3,430 cases eligible for a second interview, i.e. adjusting for the 2,138 drop-outs at Time 2. When the longitudinal weight for the 1,292 included cases is compared to the initial weight for all 3,430 cases who had a first wave interview and therefore were eligible for a second interview, the sum of the eligible weights is 3,360. This is very close to the sum of 3,362 for included cases.

A comparison of the maximum to minimum value for the initial and longitudinal weights showed that the ratio for the included cases initial weight was 15.6, compared to 13.3 for the longitudinal weight. Consequently, it was decided not to trim the longitudinal weight because the impact of outliers was expected to be no greater than when using the initial weight.

In summary, the longitudinal weight reflects the initial weight given to organisations when they were first included in the cross-sectional analysis. It does this through correcting for systematically differential loss/gain of particular organisational characteristics at the time of the second interview through the variables included in the attrition model.

Significance Testing

In the report, all longitudinal analysis refers to statistically significant changes. Two-way significance testing for longitudinal involved measuring the proportion of positive changes to negative changes between Time 1 And Time 2. This was achieved using independent groups t-test, with a two-tailed test, $p<0.05$. No adjustment was made for multiple testing.

Significance testing on the three-way tables investigated the rates of change among organisation type (medium-sized and large businesses, charities) or level of incident experienced (no incident, incident without an impact and/or outcome, incident with an impact and/or outcome). We analysed how two different groups—either marked as having a 'positive' or 'negative' flow, or 'stable'—react to specific conditions. First, we looked at the overall reaction of these groups to see if being in a positive or negative flow was statistically significant. We also considered factors such as the type of organisation they belong to or their past experiences with particular incidents. Next, we added another layer to our analysis, examining how these flows interact with those specific factors. We did this to examine if there are any unique interactions that improve our understanding of their behaviour. For example, we could test whether organisations that experienced an incident with an impact and/or outcome were more likely to invest in threat intelligence, which is a statistically significant result by this factor. We tested the accuracy of our analysis using a statistical test known as the Wald test, which helped us determine if adding these interactions provided a significant improvement to our predictive model.

Appendix A: Questionnaire

CATIINTRO
INTRO SCREEN IF CATI ONLY

Hello, my name is … from Ipsos, the independent research organisation. We are conducting a Government-sponsored survey on behalf of the Department for Science, Innovation and Technology. It is about how [SAMPLE S_INTROTEXT1] approach cyber security.

- This is the fifth year of a multi-year study.
- IF PANEL RECONTACT: You may remember, last year we interviewed you for the survey and you agreed to participate in subsequent years to take part and tell us how things have changed.
- IF FRESH SAMPLE: We may invite the same organisations back next year to take part and tell us how things have changed.
- The purpose is not to sell any software or services. It is conducted annually to generate statistics for the government.
- IF FRESH SAMPLE: We got your contact details from the [SAMPLE S_INTROTEXT2].
- Taking part is confidential.
- The interview takes an average of 20 minutes.
- Ipsos may also contact you for a separate survey related to cyber security.

IF FRESH SAMPLE OR PANEL SAMPLE BUT RESPONDENT NOT AVAILABLE

Could I please speak to the senior person at your organisation with the most responsibility when it comes to cyber security, even if they are based in a different office?

[SAMPLE S_INTROTEXT3]

[SAMPLE S_INTROTEXT4]

REASSURANCES IF NECESSARY:

- To check the survey is legitimate, details of the survey are on the GOV.UK website on https://www.gov.uk/government/publications/cyber-security-longitudinal-survey
- You can also Google the term “DSIT Cyber Longitudinal Survey” to find the same link to the GOV.UK website yourself.
- The survey helps the government to understand what guidance organisations like yours need for cyber security. Over the past years, our surveys have led to several improvements to government guidance.
- We also want to talk to organisations that have not had any cyber security issues, or that outsource their cyber security, so we get your views as well.
- The survey has been 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.

SHOW ALL OTHER STANDARD OUTCOME CODES PLUS THE FOLLOWING BESPOKE OUTCOME CODES:

- 170 – soft refusal
- 203 ineligible – wrong size in intro
- 204 ineligible – public sector at intro
- 205 ineligible – wrong size at SIZEA
- 206 ineligible – wrong size at SIZEB

REASSURANCE

READ OUT IF CATI Just so you know, this email has more information about the survey and gives you a unique link to complete all or part of the survey online, if you prefer this.

INCLUDE STANDARD REASSURANCE EMAIL SCREEN BUT WITH TEXT ABOVE ADDED

WEBINTRO

INTRO SCREEN IF WEB

Thanks for taking part in this confidential Ipsos survey about your organisation's approach to cyber security. This survey should be completed by the most senior person in the organisation who is responsible for cyber security.

Participation in the survey is voluntary and you can change your mind at any time. To check the survey is legitimate and to view Ipsos' privacy policy, you can visit the GOV.UK website on https://www.gov.uk/government/publications/cyber-security-longitudinal-survey You can also Google the term "DSIT Cyber Security Longitudinal Survey" to find the same link yourself.

As a thank you for your participation we will email you a copy of the findings [IF S_INCENTIVE = _01: and donate £15 to a charity of your choice as below].

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]

Q_INCENTIVE

ASK IF PART OF INCENTIVE GROUP (S_INCENTIVE = _01)

As promised, we will make a £15 charity donation on your behalf as a thank you for taking part. We have two charities for you to choose from:

- The NSPCC
- Samaritans

ADD IF NECESSARY:

- 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. NSPCC
2. Samaritans
3. Prefer not to donate

Screener

Q_TYPEDUM

DUMMY VARIABLE NOT ASKED

SINGLE CODE

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

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

Q_SIZEA

ASK IF BUSINESS (Q_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 SAY DK HOW BIG BUSINESS IN (Q_SIZEA = CODE 2)

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

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.

CATI: READ OUT

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 Q_SIZEA AND Q_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

Board Engagement

BOARD

READ OUT TO ALL

The first set of 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 FOR EACH STATEMENT

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: READ OUT

SINGLE CODE

1. Never
2. Once a year
3. Once every 6 months
4. Quarterly
5. Monthly
6. Weekly
7. Daily
8. Each time there is a breach or attack
9. CATI: DO NOT READ OUT: Don't know

Q_BOARDENGAGE

ASK IF BOARD DISCUSSES CYBER SECURITY (Q_BOARDDISCUSS 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_BOARDTRAINFREQ

ASK ALL

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

CATI: READ OUT

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. Board do not receive any cyber security training
6. CATI: DO NOT READ OUT: Don't know
7. 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_v3

ASK ALL

ASK AS A GRID

RANDOMISE LIST

Which of the following NCSC and DSIT information or guidance, if any, are you aware of or have you used?

CATI: READ OUT

a) The 10 Steps to Cyber Security
b) Cyber Security Toolkit for Boards
c) Cyber Aware, including top tips for staying online
d) Check your cyber security guidance
e) Cyber Governance Code of Practice
f) Software Security Code of Practice

SINGLE CODE FOR EACH STATEMENT

1. Aware, but don't currently use information/guidance
2. Aware and currently use information/guidance
3. Not Aware of information/guidance
4. CATI: DO NOT READ OUT: Don't know
5. CATI: DO NOT READ OUT: Prefer not to say

Policies, processes, and digital infrastructure within organisations

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.

Budget/Money Spent on Cyber Security

Q_CYBERSECURITYBUDGET

ASK ALL

How has the budget for cyber security changed in the last 12 months? Has it…?

CATI: READ OUT

SINGLE CODE

1. Sizeably increased
2. Somewhat increased
3. Increased in line with inflation
4. Stayed the same
5. Somewhat decreased
6. Sizeably decreased
7. CATI: DO NOT READ OUT: Don't know

Q_BUDGETCHARACTERISTIC

ASK ALL

Which of the following best characterises your cyber security budget? Is it…?

CATI: READ OUT

SINGLE CODE

1. Sufficient to address our cybersecurity needs/goals in full
2. Sufficient to address our main priorities
3. Insufficient and potentially leaving us exposed in some areas
4. Insufficient and leaving definite areas of vulnerability
5. CATI: DO NOT READ OUT: Don't know

Q_ATTITUDETOWARDSCYBERSECBUDGET

ASK ALL

Which of the following statements best describes your organisations attitude towards cyber security investment? Is it…?

CATI: READ OUT

SINGLE CODE

1. Easier to justify than other areas of the business
2. Given equivalent / fair treatment in comparison to other areas of the business
3. Harder to justify than other areas of the business
4. CATI: DO NOT READ OUT: Don't know

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

Q_REASONFORNOINSURANCE

ASK THOSE WHO DON'T HAVE A CYBER SECURITY INSURANCE POLICY IN PLACE (CODE 3 IN Q_INSUREX)

Is there a reason why you do not have cyber insurance? Is it…?

CATI: READ OUT

MULTI CODE

1. Too expensive
2. Coverage not broad enough
3. Not a budgetary priority
4. Leadership not interested in cyber insurance
5. Not aware of cyber insurance
6. CATI: DO NOT READ OUT: Don't know

Influence

Q_INFLUENCE

ASK ALL

ASK AS A GRID

RANDOMISE LIST

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
g) Another organisation in your sector experiencing a cyber security incident
h) Another organisation in your sector implementing similar measures

SINGLE CODE FOR EACH STATEMENT

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

Q_DRIVINGCHANGE

ASK ALL

RANDOMISE RESPONSES EXCEPT m AND n (WHICH SHOULD ALWAYS COME LAST)

In the last 12 months, which, if any, of the following factors have been influential in helping to improve the organisation's cyber security posture?

CATI: READ OUT

MULTICODE (EXCEPT CODE m AND o WHICH ARE SINGLE CODED)

a) Findings from a security review / assessment / test
b) Advice from Internal cyber security experts
c) Advice from external cyber security experts
d) Direct experience of cyber security incidents
e) Reports on cyber security incidents affecting others in our sector
f) Reports on cyber security incidents in general
g) Recent updates of requirements from insurers
h) Recent updates on regulatory requirements
i) Recent information received from customers / clients
j) Recent information received from partners
k) Recent information received from other stakeholders
l) There has been no notable improvement
m) Other (please specify)
n) Not sure
o) None of these

Policies and Process

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 FOR EACH STATEMENT

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)
j) A virtual private network, or VPN, for staff connecting remotely

SINGLE CODE FOR EACH STATEMENT

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 FOR EACH STATEMENT

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. Cyber Essentials
3. Cyber Essentials Plus

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

Digital infrastructure within the organisation

Q_ONLINE

ASK ALL

ASK AS A GRID

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

SINGLE CODE FOR EACH STATEMENT

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

Department for Science, Innovation and Technology	
Cyber Security Longitudinal Survey Wave Five: Technical Annex	

Processes to manage incidences

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 (Q_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 FOR EACH STATEMENT

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

Q_EXERCISE

ASK IF HAVE INCIDENT MANAGEMENT PROCESSES (Q_INCIDMAN = CODE 1)

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

SINGLE CODE

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

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 (Q_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 FOR EACH STATEMENT

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 (Q_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 FOR EACH STATEMENT

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

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.

TEXT for CAWI

The next set of questions cover 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 PREFER NOT TO SAY

a) Your organisation was asked to make a ransom payment to restore files or stop them being made public, also known as being targeted with ransomware
b) Unauthorised accessing of files or networks by staff [IF CHARITY: or volunteers], even if accidental
c) Unauthorised accessing of files or networks by people outside your organisation
d) Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services
e) Hacking or attempted hacking of online bank accounts
f) Takeovers or attempts to take over your website, social media accounts or email accounts
g) People impersonating, in emails or online, your organisation or your staff [IF CHARITY: or volunteers]
h) Phishing attacks, i.e. staff [IF CHARITY: or volunteers] receiving fraudulent emails, or arriving at fraudulent websites – even if they did not engage with these emails or websites
i) Unauthorised listening into video conferences or instant messaging

NOT PART OF RANDOMISATION

j) Others (Please Specify _____)

SINGLE CODE FOR EACH STATEMENT

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

Q_OUTCOME

ASK IF ANY CYBER SECURITY INCIDENTS (ANY Q_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 or taken by the attackers
d) Money was paid to the attackers
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 FOR EACH STATEMENT

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

Q_IMPACT

ASK IF ANY CYBER SECURITY INCIDENTS (ANY Q_INCIDENT a-k = CODE 1)

ASK AS A GRID

RANDOMISE LIST BUT KEEP A/B TOGETHER

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

CATI: READ OUT

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

SINGLE CODE FOR EACH STATEMENT

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

Admin (Re-contact Questions)

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_PANELRECON2

ASK ALL WHO SAY NO TO PANEL RE-CONTACT (Q_PANELRECON = 2)

Just to re-iterate that your input is really important. It is especially important for us to interview some organisations each year to see how things have changed.

Given the importance of your input, we really hope that you will reconsider and allow Ipsos to contact you.

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?

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 2026 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 a £70 charity donation for their time. Would you be happy to receive an invite for one of these conversations in summer/autumn 2025, if you're selected to take part?

SINGLE CODE

1. Yes
2. No

Q_NAME

ASK IF WANT RECONTACT (Q_PANELRECON = CODE 1 OR Q_PANELRECON2 = 1 OR Q_DCMSRECON = CODE 1 OR Q_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 (Q_PANELRECON = CODE 1 OR Q_PANELRECON2 = 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_TELNUMBER

ASK IF WANT DCMS OR QUAL RECONTACT (Q_QUALRECON = CODE 1 OR Q_DCMSRECON = CODE 1)

And can I please have the best telephone number to contact you about this?

WRITE IN TELEPHONE NUMBER IN VALIDATED FORMAT

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 in 2026?

SINGLE CODE

1. Yes
2. No

Q_EMAIL

ASK IF RECONTACT OR REPORT (Q_PANELRECON = CODE 1 OR Q_PANELRECON2 = CODE 1 OR Q_DCMSRECON = CODE 1 OR Q_QUALRECON = CODE 1 OR Q_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

Q_DATALINK

ASK IF ANY CYBER SECURITY INCIDENTS (ANY Q_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

Q_Consent to_share recording

Before we finish, I just want to check if you would be happy for us to share the recording of this interview with DSIT?

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. Just a reminder Ipsos may contact your organisation regarding another survey related to cyber security. 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

Introduction 2 to 3 minutes

- Introduce yourself and Ipsos: My name is *MODERATOR TO ADD NAME* and I am a researcher working for Ipsos, an independent research organisation.
- Explain research: The Department for Science, Innovation and Technology (DSIT) has commissioned Ipsos to carry out this study which involves talking to medium and large businesses and high-income charities to get a better understanding of their cyber security policies and processes. This was also covered in the Cyber Security Longitudinal Survey that took place in 2025 which you or someone in your organisation has responded to. This interview will provide an opportunity to discuss some issues in more detail.
- The interview: The discussion will be informal. There are no right or wrong answers.
- Explain confidentiality: The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties.
- Explain payment for participation. You will receive £70 as either a shopping voucher or charity donation as a thank you for your time. (*ONLY IF THEY ASK:* Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)
- Explain voluntary participation: If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary.
- Length of the interview: This discussion will last a maximum of 60 minutes.
- Questions: Do you have any questions before we begin?
- Consent to audio record: I would like to record our discussion as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely and deleted 12 months after the interview takes place.

MODERATOR TO TURN ON RECORDING

GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON)

Ipsos's legal basis for processing your data is your consent to take part in this research. Your participation is voluntary. You can withdraw your consent for your data to be used at any point before, during or after the interview and before data is anonymised at the end of September 2025.

Can I check that you are happy to proceed?

Business / charity background 2 to 3 minutes

To start our discussion, I would like to spend a few minutes understanding your business / charity in a bit more detail.

Firstly, please could you briefly describe your business / charity?

- How long has the business / charity been operating?
- What does the business / charity do?
- How would you describe the size and structure of the business / charity?

Could you briefly describe your role within the business / charity?

- How long have you been working in this business / charity?
- What are your responsibilities?

COM-B framework – Understanding the context – Capability 8 minutes

What, if any, internal or outsourced resources and or expertise does your business / charity have for managing cyber security?

- What, if any, specific internal or outsourced resources are dedicated to cyber security within your business / charity?
- Could you describe the expertise and experience levels of your internal or outsourced cyber security team?
- How, if at all, are internal or outsourced resources and or expertise secured? How are budgets secured and allocated?
- What, if any, cyber security training and or awareness programmes are available to staff?

Can you briefly describe the role, if any, that the senior leadership has in oversight for cyber security within your business/charity?

- Why do they have this role?
- What, if any, role do they have in securing budgets?
- How, if at all, often does senior leadership speak to those responsible for cyber security?

What, if any, cyber security training and or awareness programmes are available to your business' / charity's board?

MODERATOR NOTE: Training programmes are generally a structured and organised set of activities designed to develop or enhance the knowledge, skills, and competencies of individuals or groups in a specific area or subject. They tend to focus on improving employees' skill sets and are essential for supporting employees with the necessary skills, tools, and competencies to perform their roles effectively.

Awareness programmes are generally designed to educate and inform employees about specific issues, causes etc. They aim to raise awareness, trigger action, and promote understanding.

Training provides how-to knowledge and skills, while awareness programmes highlight why-it-matters.

WAIT FOR AND MAKE NOTE OF SPONTANEOUS TRAINING AND AWARENESS PROGRAMMES THEN PROMPT:

The 10 Steps to Cyber Security, Cyber Security Toolkit for Boards, Cyber Aware, Cyber Governance Code of Practice and Cyber Governance Training, ICO guidance

- *FOR TRAINING ONLY:* How often do they complete this?
- *FOR AWARENESS PROGRAMMES:* How often do you receive / participate in them?
- How do board members typically respond to the cyber security training and awareness programmes? Are there any common concerns or feedback trends?
- How effective do you believe the current cyber security training or awareness programmes are in keeping the board informed and prepared for potential cyber threats?

Can you briefly describe your business' / charity's approach to cyber risk governance and management including of supply chains?

MODERATOR NOTE: ANY TECHINCAL SOFTWARE THAT INTERVIWEES MENTION SPONTANEOUSLY.

- How, if at all, do you assess suppliers' cyber risk?

- How, if at all, do you get assurance from your suppliers? *WAIT FOR SPONTANEOUS WAYS TO EMERGE AND THEN PROMPT WITH:*
    - Supplier questionnaires
    - Contractual requirements related to cyber or product security
    - Outsourced third party/supplier risk management firms (e.g. Helios in the finance sector)
    - Bitsight or Risk Ledger (helps with continuous monitoring)
    - Certifications and standards – Cyber Essentials, ISO27001, PCIDSS (related to payments)
    - In house risk modelling based on external sources of supplier data and info
    - Adherence to GOV.UK guidance
- How, if at all, are cyber requirements built into your contracts with suppliers?
- How, if at all, are they enforced?

Does your business / charity have a list of external suppliers that it works with? This could be external suppliers that have been approved by your business / charity or those that have not gone through an approval process before their use.

MODERATOR NOTE: Those who have not gone through an approval process could have been found via online research, word of mouth, recommendation etc. without going through an approval process before use. Similarly, approved external suppliers could have been found in the same way, but they would have gone through an approval process by the organisation before use.

For example, at Ipsos' our suppliers go through a formal approval process, and once approved they make their way to the supplier database after which we can use them. – You can use this as an example to illustrate the difference.

IF YES:

MODERATOR TO MAKE A NOTE OF WHAT TYPE OF SUPPLIERS THEY WORK WITH.

- *FOR APPROVED SUPPLIERS ONLY:* How do suppliers make their way onto this list? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE ON:* Assurance measures such as compliance checks before suppliers are added to the list + refer back to the previous question
- What, if any, role do external partners play in vetting suppliers?
- How, if at all, do suppliers communicate cyber security risks with you? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE ON:* Emails, newsletters, meetings
- Are you aware of suppliers experiencing cyber security incidents? *IF YES:*
    - What, if any, impact has this had?

What, if any, are the perceived strengths of your business' / charity's cyber security capabilities?

- Why are these considered to be strengths?
- How have these come to be perceived strengths?
- *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE ON:* Whether business / charity leadership are perceived to be a strength

What, if any, are the perceived weaknesses of your business' / charity's cyber security capabilities?

- Why are these considered to weaknesses?

- How have these come to be perceived weaknesses? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE ON:* Whether business / charity leadership are perceived to be a weakness. For example, are they a barrier to securing budget and resources / do they pushback on cyber security; do they have relevant training

COM-B framework – Understanding the context – Opportunity 7 minutes

MODERATOR NOTE: THE USE OF THE TERM 'IMPROVING' AND 'IMPROVE' IN THIS SECTION ALLUDES TO FUTURE OPPORTUNITY WHEREAS THE USE OF 'MANAGING' IN THE PREVIOUS SITUATION ALLUDES TO THE CURRENT SITUATION. PLEASE CLARIFY IF NECESSARY.

What, if any, external resources, and or support is available to your business / charity for improving cyber security?

WAIT FOR SPONTANEOUS RESOURCES TO EMERGE AND THEN PROMPT: This can include information or guidance from insurance providers, contractors, suppliers, the ICO, Police and the National Cyber Security Centre (NCSC). Examples include The 10 Steps to Cyber Security, Cyber Security Toolkit for Boards, Cyber Aware, top tips for staff, Early warning service and check your cyber security , Cyber Governance Code of Practice and Software Security Code of Practice, Cyber Assessment Framework (CAF).

- What are these?
- How did you become aware of these?
- Who makes use of these within your business / charity?
- Why do you choose this particular guidance?

What, if any, best practices, or guidelines does your business / charity follow?

REFER BACK TO THE RESOURCES IN THE PREVIOUS QUESTION.

- Which, if any, of these are industry-specific?
- How did you become aware of these?
- Why are they followed?
- Briefly describe the process of how these are implemented and followed?
- Who, if anyone, is responsible for ensuring these are followed?
- How, if at all, does your business / charity assess whether suppliers follow guidelines?
- What, if any, preference does your business / charity have for following some types of practices and guidance over others? Why is this?

WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:

- Ability to operate effectively as a business / charity
- Ability to win new work as a business
- Ability to secure funding / receive donations as a charity

What, if any, are the perceived opportunities to improving cyber security within your business / charity?

- Why are these perceived to be opportunities?

WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:

- Belief that cyber security affects and impacts their business / charity
- Support from leadership such as the board within their business / charity

What, if any, are the perceived barriers to improving cyber security within your business / charity?

- Why are these perceived to be barriers?

WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:

- Belief that cyber security does not affect and impact their business / charity
- A lack of support from leadership such as the board within their business / charity

What, if any, external resources, and or support would you like to see more or less of to help your business / charity improve its cyber security?

WAIT FOR SPONTANEOUS RESOURCES TO EMERGE AND THEN PROMPT: This can include information or guidance from insurance providers, contractors, suppliers, the ICO, Police and the National Cyber Security Centre.

- Why have you suggested this?
- Who would make use of this within your business / charity?
- What, if any, impact would this have on your business / charity?

COM-B framework – Understanding the context – Motivation 6 minutes

How important, if at all, is cyber security to your business' / charities' leadership and staff?

- Why is this?
- What risk, if any, do you believe your business / charity faces from cyber security? Why is this?
- Is cyber security embedded into your organisation's wider governance structure, and if so, how?

What, if any, are the main drivers for improving cyber security attitudes within your business / charity?

- Why are these considered to be particular drivers for improving cyber security attitudes?

WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:

- Experience of cyber-attack(s) on your business
- Experience of cyber-attack(s) on your suppliers
- Potential impact of cyber-attack(s) on your business/suppliers
- Requirement for certifications such as ISO certification or Cyber Essentials as well as legislative requirements
- Regulation / GDPR / data protection – do they understand it is a legal requirement to have security measures to protect personal data?
- Requirement to meet sectoral standards
- Contractual obligations or requirements
- To retain and or win new work – and customers?
- Influencers / advisers / market actors (accountants, lawyers, banks, business contacts and networks etc), people they listen to and take advice from

What, if any, competing priorities, challenges or barriers hinder efforts to improve cyber security within your business / charity?

- Why is this?

- What, if any, impact do they have

WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:

- A lack of time
- A lack of staff
- A lack of skills
- A lack of knowledge and understanding including among leadership and those working with suppliers
- A lack of support from leadership such as the board within your business / charity
- Financial impact on budgets. *PROBE ON:* Securing budget dedicated for cyber security within the business / charity

How, if at all, does cyber security compare to other risks that your business / charity faces?

- How would you categorise this risk? For example, is it smaller, the same, or bigger?
- How have you come to make this comparison?
- Why do you take this view?

COM-B framework – Exploring influential factors – Direct experience – Behaviour 7 minutes

OPEN BROAD QUESTION: Can you please tell me about the most recent cyber security incident that your business / charity experienced?

- When did it take place? *MODERATOR NOTE*: Capture in months and or years if recall allows even if it is an estimate.
- What happened?

OPEN BROAD QUESTION: Can you please tell be about any other memorable cyber security incident(s) that your business / charity has experienced?

- When did it take place?
- What happened?
- Why was it memorable?

IF NOT ALREADY MENTIONED:

- How, if at all, have your business / charity's supply chains experienced cyber security incidents?

IF EXPERIENCED ONLY:

- When did it take place? *MODERATOR NOTE*: Capture in months and or years if recall allows even if it is an estimate.
- What happened?
- Why did it have this level of impact?

How, if at all, did the cyber security incident(s) that your business / charity experienced (*IF APPLICABLE*: including to its supply chains) impact its attitude to cyber security?

- Why did it have this level of impact?
- How, if at all, have attitudes gone back to what they were before the cyber security incident(s) that took place? Why / why not?

What, if any, specific actions were taken in response to the cyber security incident(s) that your business / charity experienced?

- Why did these actions take place?
- Who was responsible for deciding to take these actions within your business / charity?
- Who was responsible for implementing these actions within your business / charity?
- What, if any, support did you receive when implementing these actions? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Support from suppliers
    - Support from professionals

NOTE FOR MODERATORS: Other forms of support include remediation, limiting financial impact, impact mitigation, patching, vulnerability assessments (although these two should ideally take place before an incident takes place, to prevent them), data recovery, up to express support tailored to the victim organisation

- What, if any, were the costs of implementing these actions to your business / charity? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - Financial impact on budgets

What, if any, have been the longer terms effects and impacts of cyber security incident(s) that your business / charity has experienced?

- How, if at all, have processes changed? Why / why not?
- How, if at all, has investment in cyber security and or IT changed? Why / why not?
- What, if any, were the costs of implementing these actions to your business / charity? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - Financial impact on budgets

COM-B framework – Exploring influential factors – External information – Behaviour 5 minutes

Can you tell me about any cyber security incidents that you are aware of that have affected other businesses / charities in your sector?

- What were these cyber security incidents?
- How did you find out about these cyber security incidents?

How, if at all, have these cyber security incidents that affected other businesses / charities in your sector influenced your organisation's attitudes to cyber security?

- Why has it had this level of influence?

What, if any, specific actions were taken by your organisation based on other businesses / charities in your sector being affected by cyber security incidents?

IF ACTIONS WERE TAKEN:

- Why were these actions taken?
- How long after being aware of the incident were these actions taken? *PROBE ON*: How would these be categorised i.e., in the short term, medium term, or long term
- How did you come to decide taking these actions?

- Who was responsible for implementing these actions? *PROBE ON:*
- Role of the board and or business / charity leadership
- Extent to which the interviewee was responsible for taking actions or whether others such as IT, junior staff etc played a part as well the extent to which they played a part
- What level of influence did cyber security incidents affecting others have on your business / charity. For example, were cyber security incidents affecting others the sole reason that action was then taken, or did it help to provide evidence / support for existing plans or proposals?

IF NO ACTIONS WERE TAKEN:

- Why were no actions taken? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - A lack of skills
    - A lack of knowledge and understanding including among leadership and those working with suppliers
    - Financial impact on budgets
    - Belief that cyber security is already good enough
    - How did you come to decide not to take any actions?

IF NOT ALREADY MENTIONED:

How, if at all, have relationships with your supplier(s) changed based on other businesses / charities in your sector being affected by cyber security incidents?

- Why / why not?
- What, if any, influence has this had? Why? *PROBE ON:* Enforcement of requirements

COM-B framework – Exploring influential factors – Requirements and advice – Behaviour
8 minutes

Can you tell me about any recent updates to cyber security certification, or guidance or regulation, or insurer requirements that you are aware of?

- What are these?
- How did you become aware of these?

How, if at all, have these updates to certification, guidance, regulatory or insurer requirements related to cyber security impacted your business' / charities' attitudes to cyber security?

- Why has it had this level of impact?

What, if any, specific actions were taken to meet requirements in these updates?

IF ACTIONS WERE TAKEN:

- Why were these actions taken?
- How did you come to decide taking these actions?
- Who was responsible for implementing these actions?

Can you briefly describe the process of taking these actions?

- When did you start to take actions and how long did they take to enact?

- What, if any, guidance and or templates were used during this process of taking actions? Why?
- What, if any, internal policies, or procedures were created during this process of taking actions? Why?
- Did the board have a role in this process? Have they been informed about the updates?

IF NO ACTIONS WERE TAKEN:

- Why were no actions taken? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - A lack of skills
    - A lack of knowledge and understanding including among leadership and those working with suppliers
    - Financial impact of budgets
    - Belief that cyber security is already good enough
    - How did you come to decide not to take any actions?

Can you tell me about any advice that you might have sought from internal or external cyber security experts in the past 12 months?

IF ADVICE WAS SOUGHT:

- Why did you choose to seek this advice? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Experience of incidents
    - Media coverage
    - Internal advice (e.g. IT team suggests seeking external support)
- How did you decide to seek this advice?
- *IF EXTERNAL:* How did you find this advice?
- What was your experience of seeking this advice?
- What, if any, were the costs of seeking this advice? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - Financial impact on budgets

IF NO ADVICE WAS SOUGHT:

- Why have you chosen not to seek advice?
- How did you come to decide not to seek advice?
- What, if any, are barriers to you seeking advice? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - A lack of skills
    - A lack of knowledge and understanding including among leadership and those working with suppliers
    - Financial impact on budgets
    - Belief that cyber security is already good enough

IF ADVICE WAS SOUGHT: How, if at all, has this advice from internal or external cyber security experts in the past 12 months influenced your business' / charities' attitudes to cyber security?

- Why has it had this level of influence?

IF ADVICE WAS SOUGHT: What, if any, specific actions were taken based on this advice from internal or external cyber security experts?

IF ACTIONS WERE TAKEN:

- Why were these actions taken?
- How did you come to decide to take these actions?
- Who was responsible for implementing these actions?
- What, if any, were the costs of taking this action? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - Financial impact on budgets

IF NO ACTIONS WERE TAKEN:

Why were no actions taken? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*

    - Staff time
    - A lack of skills
    - A lack of knowledge and understanding including among leadership and those working with suppliers
    - Financial impact on budgets
    - Belief that cyber security is already good enough
- How did you come to decide not to take any actions?

COM-B framework – Exploring influential factors – Other factors – Behaviour 5 minutes

Can you tell me about any recent information from customers, clients, partners, suppliers, government or other stakeholders that you have received related to cyber security?

- What was this recent information?
- When did you receive it?
- Who did you receive it from?
- How was it shared?

IF RECEVIED: How, if at all, has this information influenced your business' / charities' attitude to cyber security?

- Why has it had this level of influence?

IF RECEIVED: What, if any, specific actions were taken based on this information that you have received related to cyber security?

IF ACTIONS WERE TAKEN:

- Why were these actions taken?
- How did you come to decide taking these actions?
- Who was responsible for implementing these actions?
- What, if any, were the costs of taking this action? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - Financial impact on budgets

IF NO ACTIONS WERE TAKEN:

- Why were no actions taken? *WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:*
    - Staff time
    - A lack of skills
    - A lack of knowledge and understanding including among leadership and those working with suppliers
    - Financial impact on budgets
    - Belief that cyber security is already good enough
- How did you come to decide not to take any actions?

COM-B framework – Exploring influential factors – Assessing impact – Behaviour 7 minutes

MODERATOR NOTE: FOR EACH INFLUENTIAL FACTOR IDENTIFIED THROUGHOUT THE INTERVIEW SO FAR, EXPLORE THE SPECIFIC ACTIONS TAKEN AND THEIR IMPACT ON THE ON THE BUSINESS' ATTITUDES TO CYBER SECURITY.

What, if any, were the most effective actions taken to improve cyber security within your business / charity?

- Why were these actions the most effective?

What, if any, were the least effective actions taken to improve cyber security within your business / charity?

- Why were these actions the least effective?

What, if any, challenges were encountered in implementing these actions?

- Why were these challenges?
- What was the impact of these challenges?
- How, if at all, have these challenges been overcome?

What, if any, lessons were learned from the process of improving attitudes towards cyber security within your business?

- What, if any, impact has there been of learning these lessons?

COM-B framework – Exploring influential factors – No notable improvement – Behaviour 5 minutes

MODERATOR NOTE: IF PARTICIPANTS INDICATE NO NOTABLE IMPROVEMENT IN ATTITUDES TOWARDS CYBER SECURITY, THEN EXPLORE THE REASONS BEHIND THIS.

As we come towards the end of our conversation and based on everything that we have discussed today, what if any, factors are preventing or hindering cyber security improvement efforts within your business / charity?

- Why are these factors preventing or hindering cyber security improvement efforts within your business / charity?
- WAIT FOR SPONTANEOUS REASONS TO EMERGE AND THEN PROBE WITH:
    - Staff time
    - A lack of skills

- A lack of knowledge and understanding including among leadership and those working with suppliers
- Financial impact on budgets

What, if any, are the perceived risks and consequences of not improving attitudes towards cyber security and measures to protect against cyber security incidents within your business / charity?

- How are these perceived to be risks and consequences?
- Why are these perceived to be risks and consequences?
- What, if any, impact could these perceived risks and consequences have on your business / charity?

Wrap up – ASK ALL 2 minutes

What is the key thing you would like to feed back to the Department for Science, Innovation and Technology about what we have discussed today?

Is there anything else you'd like to mention that we haven't had a chance to discuss?

The Department for Science, Innovation and Technology may want to do some follow-up research on this subject in the future. Would you be happy to be contacted by DSIT / Ipsos for future research?

INCENTIVE: Thank participant and remind them of confidentiality. Explain that they can get in touch if they have any further comments or questions about the research. Remind them of the £70 as either a shopping voucher or charity donation thank you from Ipsos, as an appreciation for their time and contribution to the research. (ONLY IF THEY ASK: Let participants know that it takes a maximum of 8 working days for them to receive the incentive.)

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.

- Colin Gardiner, Ipsos
- Jono Roberts, Ipsos
- Aamina Oughradar, Ipsos
- Shahil Parmar, Ipsos
- Jayesh Navin Shah, Ipsos
- Scott Nisbet, Ipsos
- Karl Ashworth, Ipsos

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

For general enquiries contact:

Department for Science, Innovation and Technology
22 Whitehall
London
SW1A 2EG

Telephone: 020 7211 6000

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