Department for Science, Innovation & Technology

Home Office

Official Statistics

Cyber security breaches survey 2024: technical report

Published 9 April 2024

Contents

This publication is available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-technical-report

Introduction

This Technical Annex provides the technical details of the Cyber Security Breaches Survey 2024. It covers the quantitative survey (fieldwork carried out in winter 2023 and early 2024) and qualitative element (carried out in early 2024), and copies of the main survey instruments (in the appendices) to aid with interpretation of the findings.

The annex supplements a main Statistical Release published by the Department for Science, Innovation and Technology (DSIT), covering the this year's results for businesses and charities. There is another Education Institutions Findings Annex, available on the same GOV.UK page, that covers the findings for schools, colleges and universities.

The Cyber Security Breaches Survey is a research study for UK cyber resilience, aligning with the National Cyber Strategy (https://www.gov.uk/government/publications/national-cyber-strategy-2022). It is primarily used to inform government policy on cyber security, making the UK cyberspace a secure place to do business. The study explores the policies, processes and approach to cyber security, for businesses, charities and educational institutions. It also considers the different cyber attacks and cyber crimes these organisations face, as well as how these organisations are impacted and respond.

For this latest release, the quantitative survey was carried out in winter 2023/24 and the qualitative element in early 2024.

Lead analyst

Maddy Ell

Responsible statistician

Saman Rizvi

Enquiries:

cybersurveys@dsit.gov.uk

Chapter 1: Overview

1.1 Summary of methodology

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

- We undertook a random probability telephone and online survey of 2,000 UK businesses, 1,004 UK registered charities and 430 education institutions from 7 September 2023 to 19 January 2024 (including the pilot). The data for businesses and charities have been weighted to be statistically representative of these two populations.
- We carried out 44 in-depth interviews between December 2023 and January 2024, to gain further qualitative insights from some of the organisations that answered the survey.

Sole traders and public-sector organisations were outside the scope of the survey. In addition, businesses with no IT capacity or online presence were deemed ineligible. These exclusions are consistent with previous years.

The survey methodology for this year's survey is consistent with last year's survey, but due to some changes in the questionnaire there are areas that can't be directly compared (as pointed out in the relevant sections of the main report).

1.2 Strengths and limitations of the survey overall

While there have been other surveys about cyber security in organisations in recent years, these have often been less applicable to the typical UK business or charity for several methodological reasons, including:

- focusing on larger organisations employing cyber security or IT professionals, at the expense of small organisations (with under 50 staff) that typically do not employ a professional in this role these small organisations make up the overwhelming majority of the business and charity populations
- covering several countries alongside the UK, which leads to a small sample size of UK organisations
- using partially representative sampling or online-only data collection methods.

By contrast, the Cyber Security Breaches Survey series is intended to be statistically representative of UK businesses of all sizes and all relevant sectors, and of UK registered charities in all income bands.

The 2024 survey shares the same strengths as previous surveys in the series:

- the use of random probability sampling and interviewing to minimise selection bias
- the inclusion of micro and small businesses, and low-income charities, which ensures that the respective findings are not disproportionately skewed towards larger organisations
- a data collection approach predominantly conducted by telephone, which aims to also include businesses and charities with less of an online presence (compared to online-only surveys)
- a comprehensive attempt to obtain accurate frequency and cost data from respondents, giving respondents flexibility in how they can answer (e.g. allowing numeric and banded amounts), and sending them a follow-up online survey to validate answers given in telephone interviews

- a consideration of the cost of an organisation's most disruptive cyber security breach or attack beyond the immediate direct costs (i.e. explicitly asking respondents to consider longer-term direct costs, staff time costs, as well as other indirect costs, while giving a description of what might be included within each of these cost categories).

In addition, as detailed in Section 2.1 a number of changes were made to the cyber crime questions this year to increase the accuracy of data collected.

At the same time, while this survey aims to produce the most representative, accurate and reliable data possible with the resources available, it should be acknowledged that there are inevitable limitations of the data, as with any survey project. The following might be considered the main limitations:

- Organisations can only tell us about the cyber security breaches or attacks that they have detected. There may be other breaches or attacks affecting organisations, but which are not identified as such by their systems or by staff, such as a virus or other malicious code that has so far gone unnoticed. Therefore, the survey may tend to systematically underestimate the real level of breaches or attacks. This equally applies to the cyber crime and cyber-facilitated fraud prevalence and scale estimates, given that these types of crimes emanate from cyber security breaches and attacks.
- The business survey intends to represent businesses of all sizes. As the Department for Business and Trade Business Population Estimates 2023 (https://www.gov.uk/government/statistics/business-population-estimates-2023) show, the UK business population is predominantly made up of micro and small businesses (respectively 81% and 15% of all businesses excluding sole traders). This presents a challenge these businesses, due to their smaller scale and resource limitations, typically have a less mature cyber security profile. This may limit the insights this study in isolation can generate into the more sophisticated cyber security issues and challenges facing the UK's large business population, and the kinds of high-impact cyber security incidents that appear in the news and media. Nevertheless, the study design attempts to balance this by boosting survey responses among

medium and large businesses (and high-income charities) and by focusing on larger organisations in the qualitative strand. Moreover, DSIT undertakes a separate survey series focused on larger organisations, the Cyber Security Longitudinal Survey (https://www.gov.uk/government/collections/cyber-security-longitudinal-survey), partly to address this limitation.

- Organisations may be inclined to give answers that reflect favourably on them in surveys about cyber security (a form of social desirability bias), given the common perceptions of reputational damage associated with cyber security incidents. Furthermore, organisations that have suffered from more substantial cyber security incidents may be less inclined to take part because of this. This may result in surveys like this one under-counting the true extent and cost of cyber security incidents, although we have no direct evidence of this (for example from cognitive testing). Moreover, we make a concerted effort to overcome this in the administration of the survey. We make it clear to respondents, across a range of communication materials, that their answers are confidential and anonymous.
- A significant challenge remains in terms of designing a methodology that accurately captures the financial implications of cyber security incidents, given that survey findings necessarily depend on self-reported costs from organisations. As previous years' findings and government research from 2020 on the full cost of cyber security breaches (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901569/Analysis_of_the_full_cost_of_cyber_security_breaches.pdf) suggest, there is no consistent framework across organisations at present that supports them to understand and monitor their costs, and many organisations do not actively monitor these costs at all. Moreover, we consciously opted to not to ask about certain long-term indirect costs (see Section 2.1), as it was unrealistic to collect accurate figures for these areas in a single survey. In addition, a survey based on a sample such as this one may miss some of the most financially damaging cyber security incidents, that affect a very small number of UK organisations in a very extreme way. This implies that respondents may underestimate the true economic cost of their most disruptive breaches or attacks in the survey, and that our averaged results may miss critical cases within the population. This risk of inaccuracy also applies to the cost of cyber crime estimates and provides a possible reason for the disparity

between the most disruptive cyber attack or breach and total cyber crime costs discussed in the main report.

- The total populations of further and higher education institutions available in the sample frame are small (358 and 175 respectively for this years survey). This limits the ability to achieve relatively high sample sizes among these groups. It results in much higher margins of error for the survey estimates for these groups, compared to businesses, charities and schools.

1.3 Cyber crime statistics

This year's survey produces statistics on cyber crime, and on fraud that occurs as a result of cyber crime (i.e. cyber-facilitated fraud), in UK organisations. Whilst questions on cyber crime were introduced for the first time in last year's survey, they were re-drafted this year to make questions clearer and responses more accurate. More detail on these changes can be found in section 2.1 of this annex. These changes were overseen by both DSIT and the Home Office. The survey includes estimates for:

- the prevalence of cyber crime, i.e. how many organisations are affected by them
- the nature of these cyber crimes
- the scale of cyber crimes, i.e. the number of times each organisation is impacted, and estimates for the total number of cyber crimes against UK organisations
- the financial cost of cyber crime
- a similar set of statistics with regards to frauds that occur as a result of cyber crime (cyber-facilitated fraud)

The survey approaches these estimates in a similar way to existing official estimates of crime against individuals. This includes police-recorded crime as well as the estimates from the general public Crime Survey for England and Wales (https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinengla

ndandwales/latest) (CSEW), both of which follow the Home Office Counting Rules (https://www.gov.uk/government/publications/counting-rules-for-recorded-crime). The approach aims to be as robust as possible, in the following ways:

- Comprehensiveness the questionnaire was set up to measure multiple types of cyber crime, relating to ransomware, viruses and other malware, unauthorised access to data, online takeovers, denial of service and phishing. Cyber-facilitated fraud is counted separately, as a different category of crime.
- Isolating criminal acts the survey asks a series of questions to establish whether the cyber security breaches or attacks that organisations have experienced are crimes. It systematically aims to exclude cyber attacks that were stopped by software and breaches where the organisation was not deliberately targeted (e.g. accidental accessing of confidential data by employees). It only includes phishing attacks in cases where organisations confirmed that either employees engaged in some way (e.g. by opening an attachment) or that the email contained personal data relating to the recipient and no other crimes succeeded this.
- The questions were asked in a hierarchical structure to align with the Home Office Counting Rules and ensure that where a series of attacks were inter-linked as a part of one wider incident, only one ‘principle crime’ should be recorded. For example, instances of unauthorised access may have led to subsequent events, such as ransomware, other malware or cyber-facilitated fraud. In these instances, only the ‘principle crime’ is recorded as a crime. This avoids double-counting, in line with the Home Office Counting Rules.

However, it is methodologically challenging to achieve this and as this is the first year of this version of questions, users should be relatively cautious when interpreting the statistics. For example, there is a considerable decrease between the number of businesses reporting ransomware in Chapter 4 of the main report, as an attempted or successful attack, and the number who say that the ransomware breached the organisation’s defences (i.e. was not stopped by internal security software) and as such would be classed as a crime. This is surprising as we suspect that many recipients typically would not know that a cyber attack was going to result in ransomware until the ransom is demanded, at which point systems have already been

infiltrated and a crime has been committed. We anticipate that prior to this point, any suspicious activity detected would likely be indiscernible for many businesses from a malware or unauthorised access incident, but it is possible a business could identify that they had successfully defended against a certain malware strain that was linked to ransomware. Given this uncertainty, we suggest caution in the interpretation of the statistics around ransomware and we will explore this issue further as part of next year's publication. We will also then consider whether there is value in amending any question wording in relation to either breaches, or crimes, experienced to help clarify the situation.

Furthermore, there is no baseline for comparison, so users should avoid comparison to the previous year which used a different approach. Further refinement of questions may occur next year.

The cyber crime statistics should ideally be considered alongside other, related evidence on computer misuse, such as the Crime Survey for England and Wales (https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2023) (CSEW). This survey highlighted a 30% increase in computer misuse offences against individuals in the year ending September 2023. The CSEW and Cyber Security Breaches Survey are not directly comparable, as the CSEW does not look at crime against organisations and excludes Scotland and Northern Ireland. However, it does provide a benchmark for the scale of cyber crime against individuals in England and Wales, to help contextualise the equivalent results for UK organisations in this survey.

1.4 Methodology changes from previous waves

One of the objectives of the survey is to understand how approaches to cyber security and the cost of breaches are evolving over time. Therefore, the methodology is intended to be as comparable as possible to previous surveys in the series.

As the core approach data collected from organisations via a random-probability survey, predominantly conducted by telephone is unchanged, we continue to make comparisons to previous years.

The following points cover other major changes or additions to the study that have been made in previous years:

- In the 2023 survey, the sample frame was changed for businesses from the Inter-Departmental Business Register (IDBR) to the Market Location business database. This was done to improve the overall sample quality, accuracy and telephone coverage. We did not expect this specific adaptation to have made a meaningful impact on trend findings more explanation of this is provided in Section 2.3. The sample frames for charities and education institutions were consistent with previous years (see Section 2.3).
- In the 2023 survey, we adopted a multimode data collection approach, allowing organisations to take part partially or fully online as well as by phone. This matches the approach taken in other random probability business surveys since the COVID-19 pandemic and reflects the increasing need to offer organisations the flexibility to respond online under hybrid working. More details are in Section 2.4.
- In the 2023 survey, for businesses and charities, we substantially increased the use of split-sampling where certain questions are only asked to a random half of the sample. We also restricted various questions to larger organisations (medium and large businesses, and high-income charities). Both actions were in order to maintain a questionnaire length comparable to previous years.
- The agriculture, forestry and fishing sector was included in the business sample for the first time in 2022. This is a small sector, accounting for 3.6% of all UK businesses. Its inclusion has a negligible impact on the comparability of findings across years.
- The government's 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps) guidance was refreshed between the 2022 and 2023 studies. As such, the way the 10 steps mapped to the questionnaire changed, and this section of the Statistical Release is not comparable to releases pre-2023.

- In 2021, we substantially changed the way we collect data on the costs of breaches in the survey, as part of a reflection on findings from a separate 2020 research study on the full cost of cyber security breaches (https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence). These changes mean we cannot make direct comparisons between data from 2021 onwards and previous years. We can, however, still comment on whether the broad patterns in the data are consistent with previous years, for example the differences between smaller and larger businesses, as well as charities.
- The charities sample was added in 2018, while the education institutions sample was added in 2020. The initial scope of the school and college samples were expanded from 2021 to include institutions in Wales, Scotland and Northern Ireland, as well as England.

1.5 Comparability to the pre-2016 Information Security Breaches Surveys

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

1.6 Margins of error

The survey results for businesses and charities are weighted to be representative of the respective UK population profiles for these organisations. The education institution samples are unweighted, but these groups are included as simple random samples, i.e. without any disproportionate stratification. As such, they are also considered to be representative samples. Therefore, it is theoretically possible to extrapolate survey responses to the wider population (with the exception of the financial cost data, as explained at the end of this section).

We recommend accounting for the margin of error in any extrapolated results. Table 1.1 shows the overall margins of error (MoE) for the sampled groups in the survey, for different survey estimates.

As a worked through example, the overall business sample this year has a margin of error range of ±1.6 to ±2.6 percentage points, based on a 95% confidence interval calculation. That is to say, if we were to conduct this survey 100 times (each time with a different sample of the business population), we would expect the results to be within 1.6 to 2.6 percentage points of the results we achieved here in 95 out of those 100 cases. The range illustrates that survey results closer to 50% tend to have higher margins of error. If 90% of surveyed businesses said cyber security is a high priority for their senior management, this result would have a margin of error of ±1.6 percentage points, whereas if only 50% this, the margin of error would be ±2.6 percentage points. The margins of error are calculated using the effective sample sizes (which take into account survey weighting).

For reference, we have also included MoE calculations for the split-sampled questions, where the business and charities samples are roughly half of the total. In these cases we have used the lower of the two split-samples. For example, where the business questions are split-sampled, some questions were asked to a randomly selected 1,009 business respondents (out of the total 2,000) whereas some questions were asked to the remaining 991. We have calculated the MoE for the 991.

All sample sizes shown are the unweighted totals.

Table 1.1: Margins of error (MoE) for each sample group for different survey estimates (in percentage points)

Sample group	Sample size	Effective sample size	10% or 90% estimate	30% or 70% estimate	50% estimate
Businesses	2,000	1,398	±1.6	±2.4	±2.6
Businesses - split-sampled	991	691	±2.2	±3.4	±3.7
Charities	1,004	652	±2.3	±3.5	±3.8
Charities - split-sampled	456	291	±3.4	±5.3	±5.7
Primary schools	185	185	±4.3	±6.6	±7.2
Secondary schools	171	171	±4.4	±6.7	±7.4
Further education	43	43	±8.4	±12.8	±14.0
Higher education	31	31	±9.6	±14.6	±16.0

1.7 Extrapolating results to the wider population

The total population sizes for each of these sample groups are as follows:

- 1,444,985 UK businesses with employees (according to the Department for Business and Trade Business Population Estimates 2023 (https://www.gov.uk/government/statistics/business-population-estimates-2023))
- 201,697 UK registered charities (combining the lists of registered charities across the 3 UK charity regulator databases, laid out in Section 2.3)
- 20,734 primary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 5 to 11)
- 4,486 secondary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 11+)
- 358 further education colleges
- 175 universities

As the samples for each group are statistically representative, it is theoretically possible to extrapolate survey results to the overall population. This applies both to the standard percentage estimates across the survey, and to the estimates of the scale of cyber crime and cyber-facilitated fraud (where the Statistical Release does include extrapolated estimates for the business and charity populations).

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

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

We specifically do not consider the financial cost estimates from this survey to be suitable for this sort of extrapolation (e.g. to produce a total cost of cyber incidents,

cyber crime or cyber-facilitated fraud for the UK economy). These estimates tend to have a high level of statistical standard error, so the margins of error for any extrapolated cost estimate are likely to be very wide, limiting the value of such an estimate.

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

Chapter 2: Survey approach technical details

2.1 Survey and questionnaire development

The questionnaire content is largely driven by the Cyber Resilience team at DSIT, alongside the Home Office (which has co-funded the study since 2023). They ensure that the focus aligns with the National Cyber Strategy, to provide evidence on UK cyber resilience, and influence future government policy and other interventions in this space.

Ipsos developed the questionnaire and all other survey instruments (e.g. the interview script and briefing materials) with DSIT and the Home Office. DSIT had final approval of the questionnaire. A full copy is available in Appendix A.

Development for this year's survey took place over three stages from July to September 2023:

- stakeholder engagement via email with industry representatives, and via a workshop with government representatives (alongside ongoing input over email and further meetings)
- cognitive testing interviews with 10 organisations (businesses, charities and schools)
- a pilot survey, consisting of 39 interviews (businesses, charities and schools)

Stakeholder engagement

Each year, Ipsos has consulted a range of industry stakeholders, to ensure that the Cyber Security Breaches Survey continues to explore the most important trends and themes that organisations are grappling with when it comes to cyber security. This includes the Association of British Insurers (ABI) and techUK, who were consulted this year and agreed to endorse the survey. Similarly, DSIT and the Home Office, have consulted a range of stakeholders across government, such as the National Cyber Security Centre (NCSC).

In July 2023, Ipsos facilitated a session with stakeholders from DSIT, the Home Office, the NCSC, and the devolved governments of Scotland, Wales and Northern Ireland to discuss any potential changes to the survey questionnaire. The focus was on improving the question to capture prevalence of cyber breaches and attacks, as well as the cyber crime section as a whole. Changes to these questions are listed later in this section.

Separately, Ipsos and DSIT engaged with two stakeholders that had relationships with cyber security professionals in the further and higher education sectors Jisc (a membership organisation of individuals in digital roles within the further and higher education sectors) and UCISA (https://www.ucisa.ac.uk/) (formerly known as the Universities and Colleges Information Systems Association). These organisations subsequently encouraged their members and contacts to take part in the survey, promoting the online survey link created by Ipsos (see Section 2.4).

Changes to the TYPE question

The TYPE question measures the prevalence of cyber security breaches and attacks in organisations over the past 12 months. This question is then used to route respondents into the follow-up questions covering:

- the frequency (FREQ), outcome (OUTCOME) and impact (IMPACT) of all breaches or attacks
- cyber crime and cyber-facilitated fraud (FRAUD to PHISHCONDK)
- the restoration time (RESTORE), reporting (REPORTA, REPORTB and NOREPORT), subsequent preventative measures taken (PREVENT), and costs (DAMAGEDIRS to DAMAGINDB) arising from the single most disruptive breach or attack

As a particularly central question in the survey, there have tended to be fewer changes to this question over the years. Nevertheless, the question has previously been altered on two occasions:

- Firstly, in 2017, the question was comprehensively reworded, and this version was fully or partly maintained for all subsequent years
- In 2021, there were a further set of amendments to clarify the wording in existing codes without changing the intended meaning, and to add new codes to cover potentially distinct cyber security breaches in recent years (e.g. unauthorised listening to video conferences or instant messaging, and online takeovers of websites, social media accounts and email accounts)

An equally significant set of changes were introduced in 2024:

- The overall question wording was updated to ask respondents to include all breaches or attacks, even if these had no impact (i.e. they were unsuccessful), or if they were part of a related series of breaches or attacks (e.g. in the case of an online takeover that led to ransomware, businesses were now explicitly asked to record both types of cyber attack). Whilst this had always been the intention of the question previously, it had not been made so explicit to the respondent. The

intention of this change therefore was to ensure that the question captured attempted breaches or attacks, as well as successful breaches or attacks.

- A further change to ensure that both attempted and successful breaches or attacks were captured included changing some of the text that had asked previously whether organisations had “computers becoming infected” with ransomware or other malware. Instead we asked if any devices had been “targeted” with these types of cyber attacks. This broadened the scope to include other devices such as mobile phones, and to cover unsuccessful malware that may have shown up in scans or tests.
- We added an explicit definition of ransomware within the question wording. Ransomware in the context of cyber crime specifically refers to malware that requests a ransom from the user. This definition was added to distinguish it from other types of extortion that did not explicitly involve malware. It was also added in response to potential misunderstandings in the 2023 cyber crime questions, where various respondents had suggested they had experienced ransomware, but then later said there was no specific ransom amount demanded. This suggested that respondents were conflating ransomware and other malware. Despite changes to the question this year, there is still some suggestion that we are not capturing the data as intended, as outlined in section 1.3 above. Whilst 64 businesses (after weighting was applied) said that they had experienced their organisation’s devices being targeted with ransomware, only 9 went on to say that the ransomware was not stopped by any internal or third party software. The finding that for the majority of businesses the ransomware was stopped by software highlights that respondents may not be fully understanding the question.
- We clarified that impersonation did not necessarily have to be of the organisation as a whole, but could include impersonation of staff (e.g. someone pretending to be the Chief Executive over email). The rationale for this change was that a discursive review of the questionnaire this year highlighted this omission.

The expected impact of these changes was an increase in the proportion of organisations identifying each type of breach or attack compared to previous years, given the broader scope. Therefore, we do not make direct comparisons to previous

years at this question, or at any of the questions routed from it. The same approach was taken when changes were introduced in the 2017 and 2021 questionnaires.

Overview of the cyber crime and cyber-facilitated fraud questions

The survey first added questions in 2023 to measure the prevalence, nature, scale and financial cost of cyber crime, and of the frauds that occur as a result of cyber crime. Ipsos, DSIT and the Home Office developed these questions after consulting the Office for National Statistics (ONS).

The following types of cyber crime were included:

- ransomware that breached an organisation's defences (i.e. it was not stopped by software)
- hacking attacks that were carried out deliberately, including attacks that led to extortion
- denial of service attacks that breached an organisation's defences and were carried out deliberately, including attacks that led to extortion
- computer viruses or malware other than ransomware that breached an organisation's defences
- phishing attacks that individuals engaged with (e.g. by opening an attachment) or that contained personal data about the recipient/organisation, and did not lead to any further crimes being committed

Most of these cyber crimes directly mapped to a cyber security breach or attack covered by the TYPE question. Therefore, the answers at this question were routed to the appropriate cyber crime and cyber-facilitated fraud questions. Hacking attacks mapped to three types of breaches or attacks hacking or attempted hacking of online bank accounts (code 4), unauthorised access (codes 7 and 9), and other online takeovers (code 11).

In addition, the Home Office requested the inclusion of further questions to explore the extent to which fraud occurred as a result of cyber crime. Fraud is a separate crime type (under the Fraud Act 2006) from cyber crime (which is defined in the Computer Misuse Act (https://www.legislation.gov.uk/ukpga/1990/18/contents)), but can occur following a cyber crime. This includes, for example, criminals stealing money from an organisation by:

- moving money after hacking into an organisation's online bank account
- using debit or credit card information obtained through a malware attack to make unauthorised online purchases
- getting a recipient of a phishing attack to pay or transfer money based on fraudulent information (e.g. fake invoices)

Impersonation - another type of cyber security breach or attack captured at TYPE does not, on its own, constitute a cyber crime, so new questions were added in 2024 to clarify whether the impersonation specifically occurred because of unauthorised access or other types of online takeover. In these cases, it was also treated as cyber-facilitated fraud.

There is more detail on the original development process in the 2023 Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023).

Changes to the cyber crime and cyber-facilitated fraud questions

This year, Ipsos and the Home Office extensively revised the way in which the cyber crime and cyber-facilitated fraud data was collected. The key objectives underpinning these changes were to:

- reduce the complexity of this set of questions to reduce respondent burden and obtain more accurate data
- prevent respondents from contradicting themselves, as far as possible (for example, an organisation saying they had experienced five hacking-related

incidents, but only accounting for three of these as either the principle crime or pre-cursors to other crime types, such as fraud)
- removing unnecessary text substitutions
- reducing long preambles and explanatory sentences, and moving these explanations to the exact point they were needed by respondents, if necessary
- remove double negatives, where feasible
- reduce the overall length of the questionnaire by removing questions or sample groups which did not generate enough data to be reported in 2023

Reflecting the final point above, the Home Office agreed to exclude the education institution samples from the cyber crime and cyber-facilitated fraud questions, based on the very small sample sizes.

In order to address the core objective to reduce complexity of the cyber crime questions for respondents, the questions this year were asked in a hierarchical structure. The Home Office Counting Rules (https://www.gov.uk/government/publications/counting-rules-for-recorded-crime) specify that where a series of attacks are inter-linked as a part of one wider incident, only one ‘principle crime’ should be recorded. This is typically the final event in the series of attacks. For example, if a phishing attack led to malware being installed on an organisation’s computer system and this subsequently led to criminals gaining unauthorised access to the organisation’s system using credentials obtained through the malware attack, this would be recorded as one offence of unauthorised access.

Taking a hierarchical approach, whereby the question structure dictates what should be recorded as the ‘principle crime’, means that respondents were not burdened with establishing which attack type was the ‘final event’, as they were last year. Instead, the questions were asked in the order in which we would expect the crime types to be recorded as the ‘principle crime’ if reported to the police. In the example above, respondents would be asked about how many instances of unauthorised access they experienced and then would only be asked to include any additional malware or phishing attacks they experienced which were not linked to a previous attack they had

already counted. As such, respondents should only be counting the unauthorised access, thus avoiding double counting of crimes. The hierarchy used was as follows:

1. cyber-facilitated fraud
2. successful ransomware, where this did not lead to fraud
3. deliberate unauthorised access, where this did not lead to fraud or involve ransomware
4. successful hacks of online bank accounts or other online takeovers, where these did not lead to fraud or involve ransomware
5. successful and deliberate denial of service attacks, where these did not lead to fraud or involve ransomware
6. successful malware attacks, excluding any attacks that were linked to parts 1-5 above
7. phishing attacks that individuals responded to, or that contained personal data about the recipient, excluding any attacks that were linked to parts 1-6 above

Wider questionnaire changes

The following further changes were agreed to reduce the length or improve the efficiency of the questionnaire:

- In previous years, organisations sampled as businesses had been allowed to identify as charities (since it is possible to be both a business and a registered charity). In 2024, we ceased to allow businesses to classify themselves as charities in the questionnaire (at TYPEX).
- The BARRIER question (covering the barriers to managing cyber security risks with suppliers) was removed. DSIT noted that topic would be better covered qualitatively in this or future years of the study.
- New questions were added at SCHEME to gather baseline statistics on awareness of new government guidance, including the “Check Your Cyber Security” tool on the

National Cyber Security Centre (NCSC) website, and the Cyber Action Plan for small organisations.

- The COMPLY question previously asked if organisations “adhered to” various standards like ISO 27001 and Cyber Essentials. The wording was strengthened in 2024 to specifically ask whether businesses were “certified” with these standards. As a result, we removed the statements at this question asking about the Payment Card Industry Data Security Standard (PCI DSS), and any National Institute of Standards and Technology (NIST) standards, since organisations did not gain certification for these standards.
- Based on DSIT priorities, the POLICY question (asking about the content of cyber security policies) ceased to ask about Software as a Service (SaaS) and asked for the first time in 2024 about Digital Service Providers.

Cognitive testing

The Ipsos research team carried out 10 cognitive testing interviews with businesses, charities and schools. These interviews focused on the changes to Q53A that captured the incidence of cyber attacks and breaches and the new cyber crime questions.

We recruited all participants by telephone. The sample source was organisations that took part in the previous iteration of the survey and gave permission to be recontacted for subsequent research on cyber security over the next 12 months. We applied recruitment quotas and offered an £80 incentive as a cash bank transfer to ensure participation from different-sized organisations across the country, covering a range of sectors. In addition, we asked our recruitment partner to screen all participants to ensure they had experienced at least 1 of the relevant cyber incidents achieving a minimum quota of 2 organisations covering each incident type that would enable them to answer the cyber crime questions.

The cognitive testing highlighted a few minor improvements that could be made to question wording to ease the cognitive load on respondents and ensure the questions were received consistently. These included:

- Q29A_COMPLY: an ‘add if necessary’ statement (‘By certified, we mean your organisation has applied for and received an optional certificate for meeting these standards or accreditations’) was added to the question to ensure that respondents did not become concerned they should have any of the certifications listed as a legal standard
- Q53A_TYPE: The code ‘People impersonating your organisation’ was changed to read ‘People impersonating, in emails or online, your organisation or your staff’ to avoid any potential confusion with offline impersonation
- Q53A_TYPE: The text ‘even if they did not engage with these emails or websites’ was added to the code on phishing to make explicit what had previously only been implicit
- Q56A_OUTCOME: The code ‘Money was stolen’ was changed to ‘Money was stolen or taken by the attackers’ as the cognitive interviews raised the idea that money taken or given out to attackers following a cyber attack wasn’t always perceived as ‘stolen’
- Some preambles for the cyber crime section were re-worded to avoid double negatives
- Q84A_VIRUSCOUNT and Q84B_VIRUSCOUNTDK were deleted as cognitive testing highlighted that for malware and phishing, larger organisations in particular, were going to find it hard to say how many instances, both successful and unsuccessful, had occurred in total.

As a result, Ipsos implemented these changes ahead of the survey pilot.

Pilot survey

The pilot survey was used to:

- test the questionnaire Computer-Assisted Telephone Interviewing (CATI) script
- time the questionnaire
- test the usefulness of the interviewer briefing materials

- test the quality and eligibility of the sample (by calculating the proportion of the dialled sample that ended up containing usable leads).

Ipsos interviewers carried out all the pilot fieldwork by phone between 7 and 14 September 2023. Again, we applied quotas to ensure the pilot covered different-sized businesses from a range of sectors, charities with different incomes and from different countries, and the various education institutions we intended to survey in the main fieldwork. This was with one exception we excluded any higher and further education samples, as the populations are so small (making the available sample precious). We carried out 39 interviews, breaking down as:

- 23 businesses
- 12 charities
- 4 schools (2 primary schools and 2 secondary schools)

The pilot sample came from the same sample frames used for the main stage survey (see next section). In total, the first batch of sample that was randomly selected consisted of 23,302 records.

Following the same approach as last year, the pilot was used as a soft launch of the main fieldwork. While quotas were initially applied to achieve these 39 interviews, the remaining pilot sample was subsumed into the main survey and fully worked alongside the other sample batches, following a strict random probability approach. Moreover, there were no substantial post-pilot changes to the questionnaire. Therefore, the 39 pilot interviews were counted as part of the final data.

The average interview length for the pilot was just under 23 minutes on average. Given the interview was within the target length and the questionnaire appeared to be working well, no substantive changes were made to the questionnaire following the pilot.

2.2 GOV.UK page

As in previous years, a similar GOV.UK page (https://www.gov.uk/government/publications/cyber-security-breaches-survey) 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, while the reassurance emails sent out from the CATI script (to organisations that wanted more information) included a link to the GOV.UK page.

2.3 Sampling

Business population and sample frame

The target population of businesses largely matched those included in all the previous surveys in this series, i.e. private companies or non-profit organisations[footnote 2] with more than one person on the payroll.

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

The sample frame for businesses was the Market Location database which covers businesses in all sectors across the UK at the enterprise level. It is compiled from a mix of public business directories, Companies House data and call centre activity. It is not only a clean database but also high quality; over 10,000 calls are made daily to validate numbers, with each record (telephone, email and senior contact name) having been validated within a rolling 12-month period.

Exclusions from the Market Location sample

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

In line with the previous year, businesses listed as having just 1 employee were eligible to take part in the survey (only 0-employee businesses were excluded entirely). However, given that many businesses listed as having 1 employee on business databases were found to have 0 employees, the sampling was only done on businesses listed as having 2 or more employees. This helped to avoid an unreasonably high ineligibility rate during fieldwork.

Charity population and sample frames (including limitations)

The target population of charities was all UK registered charities. The sample frames were the charity regulator databases in each UK country:

- the Charity Commission for England and Wales database: https://register-of-charities.charitycommission.gov.uk/register/full-register-download (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 (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/ (https://www.charitycommissionni.org.uk/charity-search/).

In England and Wales, and in Scotland, the respective charity regulator databases contain a comprehensive list of registered charities. DSIT was granted access to the non-public OSCR database, including telephone numbers, and a random sample of Scotland-based charities was generated.

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

Therefore, while the Charity Commission in Northern Ireland database was the best sample frame for this survey, it cannot be considered as a truly random sample of Northern Ireland charities at present. This year, there were 7,157 registered charities on the Northern Ireland database, compared to 6,880 in the 2023 survey and 6,438 in the 2022 survey.

Education institutions population and sample frame

The education institutions sample frame came from the following sources:

- all schools and colleges in England from the Get Information About Schools database (https://get-information-schools.service.gov.uk/)
- schools in Scotland from the Scottish Government School Contact details (https://www.gov.scot/publications/school-contact-details/)
- further education colleges in Scotland from the Colleges Scotland directory (https://collegesscotland.ac.uk/our-members/colleges-in-scotland)
- schools in Wales from the Welsh Government Address list of schools (https://gov.wales/address-list-schools)

- further education colleges in Wales from the Welsh Government Further Education Institutions contact details page (https://www.gov.wales/further-education-institutions-contact-details)
- schools in Northern Ireland from the Northern Ireland Department of Education database (http://apps.education-ni.gov.uk/appinstitutes/default.aspx)
- further education colleges in Northern Ireland from the NI Direct FE College directory (https://www.nidirect.gov.uk/contacts/further-education-fe-colleges)
- online lists of all UK universities, e.g. the Universities UK website (https://www.universitiesuk.ac.uk/about/Pages/member-institutions.aspx), cross-referenced against the comprehensive list of Recognised Bodies (https://www.gov.uk/check-a-university-is-officially-recognised/recognised-bodies) on GOV.UK (which also includes, for example, degree-awarding arts institutes)

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

- 20,734 primary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 5 to 11)
- 4,486 secondary schools (including free schools, academies, Local Authority-maintained schools and special schools covering children aged 11+)
- 358 further education colleges
- 175 universities

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

Business sample selection

In total, 46,777 businesses were selected from the Market Location database for the 2024 survey.

The business sample was proportionately stratified by region, and disproportionately stratified by size and sector. An entirely proportionately stratified sample would not allow sufficient subgroup analysis by size and sector. For example, it would effectively exclude all medium and large businesses from the selected sample, as they make up a very small proportion of all UK businesses according to the Department for Business and Trade Business Population Estimates 2023 (https://www.gov.uk/government/statistics/business-population-estimates-2023). Therefore, we set disproportionate sample targets for micro (2 to 10 employees), small (11 to 50 employees), medium (51 to 250 employees) and large (251 or more employees) businesses. We also boosted specific sectors, to ensure we could report findings for the same sector subgroups that were used in the 2023 report. The boosted sectors included:

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

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

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

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

SIC 2007 letter[footnote 3]	Sector description	Micro (2-10 staff)	Small (11-50 staff)	Medium (51 - 250 staff)	Large (251+ staff)	Total
A	Agriculture, forestry or fishing	1,060	173	56	40	1,329

B, C, D, E	Utilities or production (including manufacturing)	1,108	590	1,606	1,003	4,307
F	Construction	4,650	439	386	146	5,621
G	Retail or wholesale (including vehicle sales and repairs)	3,581	1,101	1,175	706	6,563
H	Transport or storage	1,015	184	425	317	1,941
I	Food or hospitality	2,935	897	704	193	4,729
J	Information or communications	1,073	319	1,127	364	2,883
K	Finance or insurance	1,262	707	1,115	518	3,602
L, N	Administration or real estate	3,228	681	1,116	1,663	6,688
M	Professional, scientific or technical	2,296	508	1,159	609	4,572
P	Education	176	55	40	926	1,197
Q	Health, social care	664	399	819	1,017	2,899

	or social work					
R, S	Entertainment, service or membership organisations	1,675	245	248	348	2,516
	Total	**24,723**	**6,298**	**9,976**	**7,850**	**48,847**

Charity and education institution sample selection

The charity sample was proportionately stratified by country and disproportionately stratified by income band, using the respective charity regulator databases to profile the population. This used the same reasoning as for businesses without this disproportionate stratification, analysis by income band would not be possible as hardly any high-income charities would be in the selected sample. In addition, having fewer high-income charities in the sample would be likely to reduce the variance in responses, as high-income charities tend to take more action on cyber security than low-income ones. This would have raised the margins of error in the survey estimates.

As the entirety of the three charity regulator databases were used for sample selection, there was no restriction in the amount of charity sample that could be used, so no equivalent to Table 2.1 is shown for charities.

Similarly, the entirety of the state education institution databases was available for sample selection, so no equivalent table is shown for education institutions.

Sample telephone tracing and cleaning

Not all the original samples were usable. In total:

- 2,118 of the 48,847 business in the original Market Location records were excluded because they had an invalid telephone number (i.e. the number was either in an

incorrect format, too long, too short, had an invalid string, or was a number which would charge the respondent when called), because they were flagged as part of Ipsos' non-contact list (organisations that have requested no further contact), or because they were based outside the UK.

- 50,524 of the 201,697 charities had no valid telephone numbers, were flagged as being on the non-contact list, or were duplicate records (i.e. with the same number appearing twice)
- 4,349 of the 25,846 education institutions had no valid telephone number or were duplicate records

We expect the unusable sample does not bias our estimates.

Ipsos undertook significant sample improvement work, using their sampling partners to match the samples to data from organisations' websites, publicly available LinkedIn pages and other social media, and Companies House data, to add in the names and job titles of relevant individuals within the business, as well as email addresses where available, in order to maximise our ability to get past gatekeepers (e.g. receptionists) and reach the appropriate individual in the organisation.

At the same time as this survey, Ipsos was also carrying out another survey with a potentially overlapping sample of businesses and charities - the DSIT cyber skills labour market survey. We therefore flagged overlapping sample leads across surveys, so telephone interviewers could avoid contacting the same organisations in quick succession for both surveys and minimise the burden on respondents. Similarly, Ipsos flagged and excluded business and charity sample leads that had recently completed Wave Three of the DSIT cyber security longitudinal survey (https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-three-results/cyber-security-longitudinal-survey-wave-three), in order to minimise the burden on respondents.

Following cleaning to remove unusable or duplicate numbers, the usable business sample amounted to:

- 46,729 business Market Location records
- 151,173 charities (with exclusions mainly due to the high prevalence of duplicate numbers in this sample frame)
- 21,404 education institutions

Table 2.2 breaks the usable business leads down by size and sector, for the business sample. As this shows, there was typically much greater telephone coverage in the medium and large businesses in the sample frame than among micro and small businesses. This has been a common pattern across previous years. In part, it reflects the greater stability in the medium and large business population, where firms tend to be older and are less likely to have recently updated their telephone numbers.

Table 2.2: Post-cleaning available business sample by size and sector (sample volumes and as a percentage of originally selected sample)

SIC 2007 letter	Sector description	Micro (2-10 staff)	Small (11-50 staff)	Medium (50 250 staff)	Large (251+ staff)	Total
A	Agriculture, forestry and fishing	1,044 (98%)	167 (97%)	56 (100%)	38 (95%)	1,305 (98%)
B, C, D, E	Utilities or production (including manufacturing)	1,099 (99%)	588 (99%)	1,572 (98%)	942 (94%)	4,201 (98%)
F	Construction	4,638 (99%)	437 (99%)	382 (99%)	142 (97%)	5,599 (99%)
G	Retail or wholesale (including vehicle	3,570 (99%)	1,097 (99%)	1,158 (99%)	668 (95%)	6,493 (99%)

	sales and repairs)					
H	Transport or storage	1,102 (99%)	183 (99%)	414 (97%)	291 (92%)	1,900 (98%)
I	Food or hospitality	2,922 (99%)	891 (99%)	688 (98%)	184 (95%)	4,685 (99%)
J	Information or communications	1,056 (98%)	310 (97%)	1,063 (94%)	324 (89%)	2,753 (95%)
K	Finance or insurance	1,240 (98%)	689 (97%)	1,055 (95%)	467 (90%)	3,451 (96%)
L, N	Administration or real estate	3,173 (98%)	659 (97%)	1,066 (96%)	1,545 (93%)	6,443 (96%)
M	Professional, scientific or technical	2,262 (99%)	492 (97%)	1,038 (90%)	526 (86%)	4,318 (94%)
P	Education	143 (81%)	40 (73%)	19 (48%)	507 (55%)	709 (59%)
Q	Health, social care or social work	606 (91%)	370 (93%)	746 (91%)	847 (83%)	2,569 (89%)
R, S	Entertainment, service or membership organisations	1,565 (93%)	227 (93%)	222 (90%)	289 (83%)	2,303 (92%)
	Total	24,330 (98%)	6,150 (98%)	9,479 (95%)	6,770 (86%)	46,729 (96%)

Sample batches

For businesses and charities, the usable sample for the main stage survey was randomly allocated into batches. The first batch, excluding the pilot sample, had 15,578 business records and 5,019 charity records.

The selection counts were modelled according to two criteria:

- If a particular size band, industry sector or (in the case of charities) income band had a higher interview target based on the disproportionate stratification, we selected more records to reflect that higher target.
- Equally, if a particular size band, industry sector or income band had historically achieved lower response rates, we selected more records to reflect these lower response rate expectations. The response rate expectations were modelled on how other recent DSIT cyber surveys using these same sample frames had performed.

For primary and secondary schools, we selected simple random sample batches of each group. In the first batch, this amounted to 1,500 primary schools and 1,500 secondary schools.

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

Subsequent sample batches were selected according to the same criteria, updated with the remaining interview targets and response rates achieved up to that point. Across all sample groups, four batches (in addition to the pilot batch) were released throughout fieldwork. We aimed to maximise the response rate by fully exhausting the existing sample batches before releasing additional records. This aim was balanced against the need to meet interview targets, particularly for boosted sample groups (without setting specific interview quotas).

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

- 32,612 Market Location records
- 7,298 charity records
- 2,050 primary schools
- 2,500 secondary schools
- 350 further education colleges
- 170 higher education institutions We did not use all the available (and usable) records for businesses, charities, primary schools and secondary schools. The remaining records were held in reserve.

2.4 Fieldwork

Ipsos carried out all main stage fieldwork from 18 September 2023 to 19 January 2024, a fieldwork period of 16 weeks.[footnote 4]

In total, we completed interviews with 3,434 organisations:

- 2,000 businesses
- 1,004 charities
- 185 primary schools
- 171 secondary schools
- 43 further education colleges
- 31 higher education institutions

The average interview length was just under c.23 minutes for all groups.

Multimode data collection

In 2023 the survey method was changed to multimode, allowing respondents to take part either by telephone or online.

In practical terms, the multimode methodology worked as follows for businesses, charities, and primary and secondary schools:

- Initial contact with organisations typically took place by phone, with Ipsos telephone interviewers calling organisations in line with previous years. The exception to this was an email invite to participate in the survey being sent out to large businesses partway through fieldwork that we hadn't been able to make contact with over the telephone.
- Where organisations requested more information before deciding to take part, interviewers could send out an information and reassurance email. This email contained a unique link for each organisation to complete the survey entirely or partially online. The interviewers explained this ahead of sending out each email.
- Beyond the initial phone call to establish contact and explain the survey, the respondents that completed the survey online had no interaction with an Ipsos interviewer when answering the questions but were instead routed through an online questionnaire, with each question appearing on a separate screen.

For further and higher education institutions, a further option was available. Ipsos created an open link to the online survey to be disseminated by Jisc and UCISA representative bodies for individuals working in IT and cyber roles in colleges and universities to their members. In total, 3 further education and 13 higher education institutions took part in the survey via this open link (and these are included in the total completed interviews mentioned at the start of Section 2.4).

In total, 149 interviews were completed using the online survey option, which represents 4% of the 3,434 total interviews. This does represent a significant drop in the online response rate from 2023, where 18% of interviews were conducted online (715 in total). There appears to be no obvious cause of this, due to the methodology remaining the same as in 2023, but is something to consider for future waves.

Table 2.3 shows how this is split across the different sample groups:

Table 2.3: Data collection mode by sample group

Sample group	Telephone interviews	Online interviews	Percentage conducted online
Businesses	1,932	68	3%
Charities	962	42	4%
Primary schools	176	9	5%
Secondary schools	158	13	5%
Further education	39	4	9%
Higher education	18	13	42%
Total	**3,285**	**149**	**4%**

Ipsos made the following efforts to monitor and maintain the quality of the online interviews, and reduce the possibility of mode differences in the responses:

- We took a best-practice approach to multimode questionnaire design, where the format of each question was similar across modes (e.g. using collapsible grids for statements online, rather than showing all statements at once). However, it should be noted that long pre-coded questions like INFO, GOVTACT, NOREPORT, REPORTB and PREVENT were unavoidably different across modes. INFO was

asked unprompted by telephone but as a prompted list online. This is standard practice in multimode questionnaires, but typically means that online respondents are inclined to give a wider range of responses (as they see a list of possible responses in front of them). This does not necessarily mean that either the telephone or online responses are wrong at any of these questions. However, it does mean that a small note of caution should be applied when comparing results for individual answer codes before and since 2023 when the multimode method was introduced.

- We validated that online respondents were the appropriate individuals from the organisation via the TITLE question (which requests job titles).
- We checked online responses to ensure respondents were not speeding through the interview or “straightlining” (i.e. answering “don’t know” or the top answer code in the list to every question).

Fieldwork preparation

Prior to fieldwork, the Ipsos research team briefed the telephone interviewing team in a video call, attended by DSIT and Home Office colleagues. They also received:

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

Screening of respondents (for telephone interviews)

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

- organisations that identified themselves as sole traders with no other employees on the payroll
- organisations that identified themselves as part of the public sector.

As this was a survey of enterprises rather than establishments, interviewers also confirmed that they had called through to the UK head office or site of the organisation.

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

For UK businesses that were part of a multinational group, interviewers requested to speak to the relevant person in the UK who dealt with cyber security at the company level. In any instances where a multinational group had different registered companies in Great Britain and in Northern Ireland, both companies were considered eligible.

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

Random probability approach and maximising participation

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

- Each organisation loaded in the main survey sample was called either a minimum of 7 times, or until an interview was achieved, a refusal given, or information obtained to make a judgment on the eligibility of that contact. In practice, our approach exceeded these minimum requirements any records marked as reaching the maximum number of tries had in fact been called 10 times or more.
- Each piece of sample was called at different times of the day, throughout the working week, to make every possible attempt to achieve an interview. Evening and weekend interviews were also offered if the respondent preferred these times.

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

- The survey had its own web page on GOV.UK, to let organisations know that the contact from Ipsos was genuine. The web pages included appropriate Privacy Notices on processing of personal data, and the data rights of participants, following the introduction of GDPR in May 2018.
- Interviewers could send a reassurance email to prospective respondents if the respondent requested this. This included a link to the GOV.UK page (https://www.gov.uk/government/publications/cyber-security-breaches-survey) to confirm the legitimacy of the survey, a link to the relevant Privacy Notice and an option to unsubscribe (by replying to the message and requesting this).
- Ipsos set up an email inbox for respondents to be able to contact to set up appointments or, in the case of the phone number, take part there and then in interviews. Where we had email addresses on the sample for organisations, we also sent five warm-up and reminder emails across the course of fieldwork to let organisations know that an Ipsos interviewer would attempt to call them and give them the opportunity to opt in by arranging an appointment. These emails also asked organisations to check the contact details we had for them and to send us better contact details if necessary. They were tailored to the type of organisation, with each email featuring a different subject line and key message to encourage participation.
- The survey was endorsed by the Association of British Insurers (ABI), the Charity Commission for England and Wales and the Charity Commission for Northern Ireland and techUK. In practice, this meant that these organisations allowed their identity and logos to be used in the survey introduction and on the microsite, to encourage organisations to take part.
- Specifically, to encourage participation from colleges and universities, DSIT and Ipsos jointly worked with Jisc and UCISA. These organisations contacted their members, which include IT and cyber security professionals in the further and higher education sectors, to proactively ask them to take part in the survey via the open link.

- Large businesses were offered a £10 charity donation on their behalf if they took part. They could choose to donate to Turn2us, the NSPCC or the Samaritans.

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.

Recontact survey to clarify responses at cyber breaches and attacks cost questions

During the main fieldwork period in 2023, Ipsos, DSIT and the Home Office developed a recontact survey to revalidate some of the cost of breaches data that respondents had provided in the survey. This acted as a second check on the numeric data to ensure it hadn't been inputted incorrectly.

In total, 1,105 businesses were eligible for being sent the link to the validation and 970 of these agreed for it to be sent. Only 33 respondents took part in the validation survey and following the answers given at this survey only one edit was made to the data at question 'damagestaff'.

Based on low uptake of the validation survey and a high level of accuracy in the data that is provided, a review is recommended as to whether the validation survey should continue to be used in future waves.

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, the response rate and the response rate adjusted for unusable or ineligible records, for businesses and charities. The approach for calculating these figures is covered later in this section.

Table 2.4: Fieldwork outcomes and response rate calculations for businesses and charities

Outcome	Businesses	Charities
Total selected from original sample frame	48,847	201,697
Sample without contact details or duplicates post-cleaning	2,118	50,524
Net: total sample with contact details	**46,729**	**151,173**
Sample with contact details left in reserve	14,117	143,875
Net: total sample used (i.e. excluding any left in reserve)	**32,612**	**7,298**
Unresponsive numbers	13,844	3,341
Refusals	5,853	831
Unusable leads with working numbers	550	119
Unusable numbers	3,843	1,172
Ineligible leads - established during screener	659	235

Incomplete interviews	5,804	617
Net: completed interviews	**2,000**	**1,004**
Expected eligibility of screened respondents	92%	97%
Response rate	**6%**	**14%**
Response rate adjusted for unusable or ineligible records	**7%**	**17%**

The fieldwork outcomes for state education institutions are shown in Table 2.5.

Table 2.5: Fieldwork outcomes and response rate calculations for state education institutions

Outcome	Primary schools	Secondary schools	Further education	Higher education
Total selected from original sample frame	20,734	4,486	488	175
Sample without contact details or duplicates post-cleaning	3,598	738	8	5
Net: total sample with contact details	**17,136**	**3,748**	**480**	**170**
Sample with contact	15,086	1,248	130	0

details left in reserve				
Net: total sample used (i.e. excluding any left in reserve)	**2,050**	**2,500**	**350**	**170**
Incomplete interviews	1,664	1,831	306	138
Ineligible leads - established during screener	23	41	7	3
Refusals	125	92	14	8
Unusable leads with working numbers	9	12	1	4
Unusable numbers	92	82	18	9
Unresponsive numbers	3	1	0	0
Net: completed interviews	**185**	**171**	**43**	**31**
Expected eligibility of screened respondents	98%	97%	100%	100%
Response rate	**9%**	**7%**	**12%**	**18%**
Response rate adjusted for unusable or ineligible records	**9%**	**8%**	**12%**	**18%**

Notes on response rate calculations

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

- Response rate = completed interviews / total sample used
- Response rate adjusted for unusable or ineligible records = completed interviews / (completed interviews + incomplete interviews + refusals expected to be eligible + any remaining unresponsive numbers expected to be eligible)
- Refusals exclude “soft” refusals. This is where the respondent was hesitant about taking part, so our interviewers backed away and avoided a definitive refusal.
- Unusable leads with working numbers are where there was communication difficulty making it impossible to carry out the survey (e.g. a bad line, or language difficulty), as well as numbers called 10 or more times over fieldwork without ever being picked up.
- Unusable numbers are where the number was in a valid format, so was loaded into the main survey sample batches, but which turned out to be wrong numbers, fax numbers, household numbers or disconnected.
- Unresponsive numbers account for sample that had a working telephone number, but where the respondent was unreachable or unavailable for an interview during the fieldwork period, so eligibility could not be assessed.

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

The adjusted response rates for all the sampled groups, outside of higher education institutions, are lower than in earlier iterations of this study, that took place before the COVID-19 pandemic. For example, the adjusted response rates for the last survey in this series that took place before the pandemic (CSBS 2020) were 27% for businesses and 45% for charities.

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

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

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

Furthermore, the increase in the survey length from c.17 minutes in 2020 and earlier iterations, to just under 23 minutes last year is also expected to have reduced the response rate interviewers must mention the average length to respondents when they introduce the survey, and respondents are naturally less inclined to take part in longer interviews.

To a lesser extent, the existence of another DSIT organisational survey on cyber security, the Cyber Security Longitudinal Survey (https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-two-results) (CSLS), may have impacted the performance of this survey. Ipsos also undertook fieldwork for the CSLS. The CSLS fieldwork took place earlier than for CSBS, between March and June 2023. Organisations that took part in the CSLS were excluded from the sample for the Cyber Security Breaches Survey. However, organisations that were contacted for that survey but opted not to take part may also have been resampled and contacted anew for the Cyber Security Breaches Survey and been less likely to take part as a result.

However, it is important to remember that response rates are not a direct measure of non-response bias in a survey, but only a measure of the potential for non-response bias to exist. Previous research into response rates, mainly with consumer surveys, has indicated that they are often poorly correlated with non-response bias.[footnote 5]

2.6 Data processing and weighting

Editing and data validation

There were a number of logic checks in the CATI script, which checked the consistency and likely accuracy of answers estimating costs and time spent dealing with breaches. If respondents gave unusually high or low answers at these questions relative to the size of their organisation, the interviewer would read out the response they had just recorded and double-check this is what the respondent meant to say. In addition, respondents overwhelmingly revalidated their answers at the cost questions in the online follow-up survey. This meant that, typically, minimal work was needed to manually edit the data post fieldwork.

Coding

The verbatim responses to unprompted questions could be coded as “other” by interviewers when they did not appear to fit into the predefined code frame. These “other” responses were coded manually by Ipsos’ coding team, and where possible, were assigned to codes in the existing code frame. It was also possible for new codes to be added where enough respondents 10% or more had given a similar answer outside of the existing code frame. The Ipsos research team verified the accuracy of the coding, by checking and approving each new code proposed.

The codeframe between 2023 and 2024 has remained consistent.

We did not undertake SIC coding. Instead the SIC 2007 codes that were already in the IDBR sample were used to assign businesses to a sector for weighting and analysis purposes. The pilot survey in 2017 had overwhelmingly found the SIC 2007 codes in the sample to be accurate, so this practice was carried forward to subsequent surveys.

Significant differences

When reporting on sub-groups, we note whether or not results from sub-groups differ in a statistically significant way. Statistical significance testing is used to determine whether differences in results are likely to be due to a genuine difference between groups, as opposed to chance variation. The threshold used in the main report is the 95% level of confidence, meaning there is less than a 5% chance that results deemed significantly different differ due to chance. This is a standard level of significance used in social sciences. The test used to determine statistical significance is a two-tailed t-test.

Weighting

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

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

Rim weighting is a standard weighting approach undertaken in business surveys of this nature, because it allows you to weight your sample to represent a wider population using multiple variables. In cases where the weighting variables are strongly correlated with each other, it is potentially less effective than other methods, such as cell weighting. However, this is not the case here.

We did not weight by region, primarily because region is not considered to be an important determining factor for attitudes and behaviours around cyber security. Moreover, the final weighted data are already closely aligned with the business population region profile. The population profile data came from the Department for

Business and Trade Business Population Estimates 2023 (https://www.gov.uk/government/statistics/business-population-estimates-2023).

Non-interlocking rim weighting by income band and country was undertaken for charities. The population profile data for these came from the respective charity regulator databases.

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

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

Table 2.6: Unweighted and weighted sample profiles for business interviews

	Unweighted %	Weighted %
Size		
Micro (1 - 9 staff)	53%	82%
Small (10 - 49 staff)	25%	15%
Medium (50 - 249 staff)	13%	3%
Large (250+ staff)	9%	1%
Sector		

Agriculture, forestry or fishing	4%	4%
Administration or real estate	13%	13%
Construction	11%	14%
Education	2%	2%
Entertainment, service or membership organisations	6%	7%
Finance or insurance	7%	2%
Food or hospitality	8%	10%
Health, social care or social work	6%	4%
Information or communications	6%	5%
Professional, scientific or technical	11%	13%
Retail or wholesale (including vehicle sales or repairs)	15%	17%
Transport or storage	4%	4%
Utilities or production (including manufacturing)	8%	7%

Table 2.7: Unweighted and weighted sample profiles for charity interviews

	Unweighted %	Weighted %

Income band		
£0 to under £10,000	28%	43%
£10,000 to under £100,000	19%	34%
£100,000 to under £500,000	20%	15%
£500,000 to under £5 million	18%	6%
£5 million or more	16%	2%
Country		
England and Wales	91%	84%
Northern Ireland	3%	4%
Scotland	6%	12%

2.7 SPSS data uploaded to UK Data Archive

A de-identified SPSS dataset from this survey is being published on the UK Data Archive to enable further analysis. The variables are largely consistent with those in the previously archived dataset (from 2023), outside of deleted questions and the new cyber crime questions.

Mapping of 10 Steps guidance

As noted in Section 2.1, Ipsos engaged Professor Steven Furnell from the University of Nottingham in July 2022 to review how the questionnaire was mapped to the government's 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps) guidance, and suggest a more accurate and robust mapping. The 10 Steps mapping remains consistent with 2023 and is outlined in Table 2.8.

Table 2.8: Mapping of the questionnaire to the 10 Steps to Cyber Security guidance

Step in SPSS	Current step description and mapping
Step 1	Risk management - organisation have undertaken a cyber security risk assessment (IDENT4)
Step 2	Engagement and training - staff receive cyber security training (TRAINED)
Step 3	Asset management - organisations have a list of their critical assets (MANAGE8)
Step 4	Architecture and configuration - organisations have at least 3 of the following: up-to-date malware protection (RULES2) firewalls that cover your entire IT network, as well as individual devices (RULES3) restricting IT admin and access rights to specific users (RULES4) security controls on organisation-owned devices (e.g. laptops) (RULES7) only allowing access via organisation-owned devices (RULES8) separate WiFi networks for staff and for visitors (RULES9) specific rules for storing and moving personal data files securely (RULES15) a virtual private network, or VPN, for staff connecting remotely (RULES18)

Step 5	Vulnerability management - organisations have policy to apply software security updates within 14 days (RULES1)
Step 6	Identity and access management - organisations have any requirement for two-factor authentication when people access the organisation’s network, or for applications they use (RULES20)
Step 7	Data security - organisations have cloud backups (RULES13) or other kinds of backups (RULES14)
Step 8	Logging and monitoring organisations fulfil at least 1 of the following criteria: used specific tools designed for security monitoring, such as Intrusion Detection Systems (IDENT11) any monitoring of user activity (RULES5)
Step 9	Incident management - organisations have a formal incident response plan (INCIDCONTENT1) or at least 3 of the following: written guidance on who to notify of breaches (INCIDCONTENT2) roles or responsibilities assigned to specific individuals during or after an incident (INCIDCONTENT3) external communications and public engagement plans (INCIDCONTENT6) guidance around when to report incidents externally, e.g. to regulators or insurers (INCIDCONTENT11)
Step 10	Supply chain security - organisations have taken actions to manage the cyber risks from their immediate suppliers (SUPPLYRISK1) or wider supply chain (SUPPLYRISK2)

Organisation size variables

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

Sector grouping before the 2019 survey

In the SPSS datasets for 2016 to 2018, an alternative sector variable (sector_comb1) was included. This variable grouped some sectors together in a different way, and was less granular than the updated sector variable (sector_comb2).

- “education” and “health, social care or social work” were merged together, rather than being analysed separately
- “information or communications” and “utilities” were merged together, whereas now “utilities” and “manufacturing” are merged together.

The previous grouping reflected how we used to report on sector differences before the 2019 survey. As this legacy variable has not been used in the report for the last two years, we have stopped including it in the SPSS dataset, in favour of the updated sector variable.

Derived financial cost estimates for cyber security breaches and attacks

For the questions in the survey estimating the financial costs of an organisation’s most disruptive breach or attack (DAMAGEDIRSX, DAMAGEDIRLX, DAMAGESTAFFX, DAMAGEINDX), respondents were asked to give either an approximate numeric response or, if they did not know, then a banded response. The vast majority of those who gave a response gave numeric responses (after excluding refusals and those saying there was no cost incurred).

We agreed with DSIT from the outset of the survey that for those who gave banded responses, a numeric response would be imputed, in line with all previous surveys in

the series. This ensures that no survey data goes unused and also allows for larger sample sizes for these questions.

To impute numeric responses, syntax was applied to the SPSS dataset which:

- calculated the mean amount within a banded range for respondents who had given numeric responses (e.g. a £200 mean amount for everyone giving an answer between £100 and £500)
- applied this mean amount as the imputed value for all respondents who gave the equivalent banded response (i.e. £200 would be the imputed mean amount for everyone not giving a numeric response but saying “£100 to less than £500” as a banded response).

Often in these cases, a common alternative approach is to take the mid-point of each banded response and use that as the imputed value (i.e. £300 for everyone saying “£100 to less than £500”). It was decided against doing this for these specific questions, given that the mean responses within a banded range have tended to cluster towards the bottom of the band over the years. This suggested that imputing values based on mid-points would slightly overestimate the true values across respondents.

Derived cyber crime estimates (including numeric and financial cost estimates)

There are a range of new derived variables in this year’s SPSS file based on the cyber crime questions. Here is a brief description of each derived variable:

- Cybercrime_all the percentage of organisations that have experienced any cyber crime (i.e. excluding cyber-facilitated fraud)
- Cybercrime_allsum the total number of cyber crimes experienced (i.e. excluding cyber-facilitated fraud), rebased to only be amongst those that experienced cyber crimes
- Cybercrime_notphish the percentage of organisations that have experienced any cyber crime other than phishing (still excluding cyber-facilitated fraud)

- Cybercrime_notphishsum the total number of cyber crimes experienced, other than phishing (still excluding cyber-facilitated fraud), rebased to only be amongst those that experienced these cyber crimes
- Cybercrime_rans the percentage of organisations that have experienced cyber crime relating to ransomware
- Cybercrime_ranssum the total number of cyber crimes experienced relating to ransomware, rebased to only be amongst those that experienced these cyber crimes
- Cybercrime_virus the percentage of organisations that have experienced cyber crime relating to viruses or other malware
- Cybercrime_virussum the total number of cyber crimes experienced relating to viruses or other malware, rebased to only be amongst those that experienced these cyber crimes
- Cybercrime_hack the percentage of organisations that have experienced cyber crime relating to hacking
- Cybercrime_hacksum the total number of cyber crimes experienced relating to hacking, rebased to only be amongst those that experienced these cyber crimes
- Cybercrime_dos the percentage of organisations that have experienced cyber crime relating to denial of service attacks
- Cybercrime_dossum the total number of cyber crimes experienced relating to denial of service attacks, rebased to only be amongst those that experienced these cyber crimes
- crime_fraud the percentage of organisations that have experienced fraud as a result of cyber crime
- crime_fraudsum the total number of frauds experienced as a result of cyber crime, rebased to only be amongst those that experienced these frauds
- Cybercrime_phish the percentage of organisations that have experienced cyber crime relating to phishing
- Cybercrime_phishsum the total number of cyber crimes experienced relating to phishing, rebased to only be amongst those that experienced these cyber crimes

- Extortion the percentage of organisations that have experienced any extortion (among those experiencing cyber crimes relating to unauthorised access, online takeovers or denial of service)
- Extortion_sum the total number of extortion events, rebased to only be amongst those that experienced cyber crimes relating to unauthorised access, online takeovers or denial of service
- hacksumcost_bands the total cost of criminal hacking and online takeovers in the last 12 months, rebased to only be amongst those that provided a cost estimate for any relevant cyber crime experienced
- notfraudcost_bands the total cost of all cyber crimes (i.e. excluding cyber-facilitated fraud), rebased to only be amongst those that provided a cost estimate for any relevant cyber crime experienced
- fraudcost_bands the total cost of fraud that occurred as a result of cyber crime
- crimecost_bands the total cost of all crimes (including cyber-facilitated fraud), rebased to only be amongst those that provided a cost estimate for any crime experienced.

For the numeric and financial cost estimates for cyber crime, respondents were also able to give a banded response if they could not provide an exact answer. We have opted to impute the numeric or financial value for these questions by taking the mid-point of each banded response (or the specific value mentioned in the top band). This is different from the cyber incident cost estimates, which impute the average value within the band. The sample of cyber crime cost estimates is much lower, so there is not enough data to impute average values within bands. In other words, it is simply not possible to use anything other than the mid-point values.

Redaction of financial cost estimates in published SPSS data

No numeric cost variables will be included in the published SPSS dataset, both for the cyber incident (DAMAGE) questions and the crime (COSTA) questions. This was agreed with DSIT to prevent any possibility of individual organisations being identified.

Instead, all variables related to spending and cost figures will be banded, including the imputed values (laid out in the previous section). These banded variables include:

- damagedirsx_bands
- damagedirlx_bands
- damagestaffx_bands
- damageindx_bands
- damage_bands
- ransdem_bands
- ranspay_bands
- ranscost_bands
- viruscost_bands
- hackcost_bands
- tkvrcost_bands
- doscost_bands
- fraudcost_bands2
- hacksumcost_bands
- notfraudcost_bands
- fraudcost_bands
- crimecost_bands.

In addition, the following merged or derived variables will be included:

- country_comb
- ext_report
- scheme_any
- supplyrisk_any
- supplycert_any

- type6x
- morethanphish
- disruptax

No region groupings are included for the education institution data, to avoid the risk of these schools, colleges or universities being identified.

Missing values

We have treated missing values consistently each year.

- For all non-cost data, only respondents that did not answer a question are treated as missing, and allocated a value of -1. That means that all responses, including “don’t know” (a value of -97) and “refused” responses (-99) are counted in the base and in any descriptive statistics.
- For all cost data, i.e. damagedirs through to cost_bands, the “don’t know” (-97) and “refused” (-99) responses are treated as missing. Practically, this means that any analysis run on these variables systematically excludes “don’t know” and “refused” responses from the base. In other words, this kind of analysis (e.g. analysis to show the mean cost or median cost) only uses the respondents that have given a numeric or banded cost.

Rounding differences between the SPSS dataset and published data

If running analysis on weighted data in SPSS, users must be aware that the default setting of the SPSS crosstabs command does not handle non-integer weighting in the same way as typical survey data tables.[footnote 6] Users may, therefore, see very minor differences in results between the SPSS dataset and the percentages in the main release, which consistently use the survey data tables. These should be differences of no more than one percentage point, and only occur on rare occasions.

Chapter 3: Qualitative approach technical details

The qualitative strand of this research covered all the sampled groups from the survey. We conducted 44 in-depth interviews overall, the same as in 2023.

3.1 Sampling

We took the sample for all 44 in-depth interviews from the quantitative survey. We asked respondents during the survey whether they would be willing to be recontacted specifically to take part in a further 60-minute interview on the same topic. Table 3.1 shows the proportion of respondents from each group that agreed to be recontacted, the total recontact sample available, and the qualitative interviews undertaken with each group.

Table 3.1: Summary of qualitative sample counts and interviews

Sample group	Achieved quantitative interviews	Permission for recontact	Recontact sample	Achieved qualitative interviews
Businesses	2,000	63%	1,256	20
Charities	1,004	62%	627	10
Primary schools	185	59%	109	5

Secondary schools	171	61%	105	1
Further education	43	49%	21	4
Higher education	31	55%	17	4

3.2 Recruitment quotas and screening

We carried out recruitment for the qualitative element by email and telephone, using the contact details collected in the survey, and via a specialist business recruiter. We offered a high street voucher or charity donation of £50 made on behalf of participants to encourage participation.

We used recruitment quotas to ensure that interviews included a mix of different sizes, sectors and regions for businesses, and different charitable areas, income bands and countries for charities. We also had further quotas based on the responses in the quantitative survey, reflecting the topics to be discussed in the interviews. These ensured we spoke to a range of organisations that had:

- a formal cyber security strategy
- adopted specific cyber security standards or accreditations
- formally reviewed supply chain cyber security risks (including for immediate suppliers and their wider supply chain)
- some form of incident response planning
- referenced their cyber security risks in a corporate annual report

- used Managed Service Providers or other Digital Service Providers
- identified cyber security breaches

These were all administered as soft rather than hard quotas. This meant that the recruiter aimed to recruit a minimum number of participants in each group, and could exceed these minimums, rather than having to reach a fixed number of each type of respondent.

We also briefed the recruiter to carry out a further qualitative screening process of participants, to check that they felt capable of discussing at least some of the broad topic areas covered in the topic guide (laid out in the following section). The recruiter probed participants' job titles, job roles, and gave them some further information about the topic areas over email. The intention was to screen out organisations that might have been willing to take part but would have had little to say on these topics.

3.3 Fieldwork

The Ipsos research team carried out all fieldwork in December 2023 and January 2024. We conducted the 44 interviews through a mix of telephone and Microsoft Teams calls. Interviews lasted around 60 minutes on average.

DSIT and the Home Office originally laid out their topics of interest for the 2024 study. Ipsos then drafted the interview topic guide around these topics, which was reviewed and approved by both departments. The qualitative topic guide has changed slightly each year, in order to respond to the new findings that emerge from each year's quantitative survey. The intention is for the qualitative research to explore new topics that were not necessarily as big or salient in previous years, as well as to look more in depth at the answers that organisations gave in this year's survey. This year, the guide covered the following broad thematic areas:

- perception of cyber security risk
- impact of economic uncertainty on cyber security investment and prioritisation
- cyber security leadership and governance (including roles of board members, risk management and incident planning)
- incidence response
- corporate annual reporting on digital strategy and risks
- digital service providers
- cyber security practices (privacy enhancing technologies, standards and accreditations and supply chain decisions)

There was not enough time in each interview to ask about all these topics, so we used a modular topic guide design, where the researcher doing the interview would know beforehand to only focus on a selection of these areas. Across the course of fieldwork, the core research team reviewed the notes from each interview and gave the fieldwork team guidance on which topics needed further coverage in the remaining interviews. This ensured we asked about each of these areas in a wide range of interviews, with at least 4 interviews covering each topic.

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

Tables 3.2 and 3.3 shows a profile of the 20 interviewed businesses by size and sector.

Table 3.2: Sector profile of businesses in follow-up qualitative stage

SIC 2007 letter	Sector description	Total
A	Agriculture, forestry or fishing	0
B, C, D, E	Utilities or production (including manufacturing)	2

F	Construction	1
G	Retail or wholesale (including vehicle sales and repairs)	2
H	Transport or storage	1
I	Food or hospitality	0
J	Information or communications	2
K	Finance or insurance	1
L, N	Administration or real estate	1
M	Professional, scientific or technical	4
P	Education (excluding state education institutions)	0
Q	Health, social care or social work	4
R, S	Entertainment, service or membership organisations	2
	Total	20

Table 3.3: Size profile of businesses (by number of staff) in follow-up qualitative stage

Size band	Total
Micro or small (1 - 49 staff)	6

Medium (50 - 249 staff)	7
Large (250+ staff)	7
Total	20

Table 3.4 shows a profile of the 10 interviewed charities by income band.

Table 3.4: Size profile of charities (by income band) in follow-up qualitative stage

Income band	Total
£100,000 to under £500,000	2
£500,000 to under £5 million	3
£5 million or more	5
Total	10

3.4 Analysis

Throughout fieldwork, the core research team discussed interim findings and outlined areas to focus on in subsequent interviews. Specifically, we held two face-to-face analysis meetings with the entire fieldwork team one halfway through fieldwork and one towards the end of fieldwork. In these sessions, researchers discussed the

findings from individual interviews, and we drew out emerging key themes, recurring findings and other patterns across the interviews. DSIT and the Home Office attended a separate analysis session during the latter part of fieldwork and helped identify key findings, as well as areas worth exploring further in the remaining interviews.

We also recorded all interviews and summarised them in an Excel notes template, which categorised findings by topic area and the research questions within that topic area. The research team reviewed these notes, and also listened back to recordings, to identify the examples and verbatim quotes to include in the main report.

Chapter 4: Research burden

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

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

- The quantitative survey had 3,434 respondents and the average (mean) survey length was 23 minutes. There was a further recontact survey of 13 respondents, lasting an average of 5 minutes. Therefore the research compliance cost for the quantitative survey this year was [(3,434 × 23 minutes) + (13 × 5 minutes) = 1,317 hours].
- The qualitative research had 44 respondents and the average interview length was 60 minutes. Respondents completed the qualitative interviews in addition to the

quantitative survey. The research compliance cost for the qualitative strand this year was [44 × 60 minutes = 44 hours].

In total, the compliance cost for the Cyber Security Breaches Survey 2024 was 1,361 hours.

Steps taken to minimise the research burden

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

- making it clear that all participation was voluntary
- informing respondents of the average time it takes to complete an interview at the start of the survey call, during recruitment for the qualitative research and again at the start of the qualitative interview
- confirming that respondents were happy to continue if the interviews went over this average time
- split-sampled certain questions that is to say they were asked to a random half of respondents to reduce the overall interview length
- offering to carry out interviews at the times convenient for respondents, including evenings and weekends where requested
- offering an online interview instead of a telephone one, according to the respondent's preferences.

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

Appendix A: Questionnaire

Cyber Security Breaches Survey 2024
Main stage questionnaire

Key

INTERVIEWER INSTRUCTIONS IN CAPS

Screener

CATIINTRO
INTRO SCREEN IF TELEPHONE (MODETYPE = CATI)
Is this the head office for [SAMPLE CONAME]?

IF NOT THE HEAD OFFICE, ASK TO BE TRANSFERRED AND RESTART

Hello, my name is … from Ipsos, the independent research organisation.

IF CALLING 08 NUMBER FOR CHARITY (SAMPLE S_FREENUM=_01): Before I proceed, I'd like to make clear that I'm calling your 0800 number, for which you may be charged. Would you like me to proceed, or call on a different number?

We are conducting a survey on behalf of [SAMPLE S_COUNTRY=_03: the Department for Science, Innovation and Technology, the Home Office and Scottish Government/ELSE: the Department for Science, Innovation and Technology and the Home Office]. It is about how UK [SAMPLE S_SAMPTYPE=_01: businesses/SAMPLE S_SAMPTYPE=_02: charities/SAMPLE S_SAMPTYPE=_03: education institutions] of all different sizes approach cyber security and online safety. Each year, the organisations that take part help to shape the government's guidance on this topic.

- [SAMPLE S_SIZEBAND=_04: If your organisation takes part, Ipsos will make a £10 donation to charity on your behalf at the start of the interview.]

- The purpose is not to sell any software or services. It is conducted annually to generate Official Statistics for the Government.
- Taking part is confidential.
- The interview takes an average of 20-22 minutes, and is typically shorter for smaller organisations.
- The organisations that take part get given a summary of last year's findings, as well as a help card with links to the latest Government cyber security guidance for [SAMPLE S_SAMPTYPE=_01: businesses/SAMPLE S_SAMPTYPE=_02: charities/SAMPLE S_SAMPTYPE=_03: education institutions].

Could I please speak to the senior person at your organisation with the most responsibility when it comes to cyber security?

IF OUTSOURCE CYBER SECURITY: In that case, we want to talk to the person within your organisation who typically deals with your external IT or cyber security provider. We know this may be the business owner, a trustee, Chief Executive, or someone else from the senior management team.

REASSURANCES IF NECESSARY

- We got your contact details from the [SAMPLE S_SAMPTYPE=_01: Market Location business database/SAMPLE S_COUNTRY=_01: Charity Commission for England and Wales/SAMPLE S_COUNTRY=_02: Charity Commission for Northern Ireland/SAMPLE S_COUNTRY=_03: Office of the Scottish Charity Regulator/SAMPLE S_SAMPTYPE=_03: public databases of schools, colleges and universities].
- The survey is for all types of businesses and charities. 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 is not technical we want your views, not just expert opinion on this topic.
- The survey has been endorsed by techUK, the Association of British Insurers (ABI), and the Charity Commission for England and Wales.

- To check the survey is legitimate, you can visit the GOV.UK website on www.gov.uk/government/publications/cyber-security-breaches-survey. You can also Google the term “Cyber Security Breaches Survey 2024” to find the same link yourself.

SHOWSCREEN_REASSURANCE
SHOW IF TELEPHONE (MODETYPE = CATI) AND WANTS REASSURANCE EMAIL
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. We may call you back after a few days to help you get the survey completed, if you’re unable to fill it out online.

STANDARD OPTIONS TO SEND REASSURANCE EMAIL

WEBINTRO
INTRO SCREEN IF WEB (MODETYPE = WEB/ONLINE)
Thanks for filling in this important government survey. This survey should be completed by the most senior person in the organisation who is responsible for cyber security.

Each year, the organisations that take part help to shape the government’s guidance on cyber security and online safety.

[SAMPLE S_SIZEBAND=_04: If your organisation takes part, Ipsos will make a £10 donation to charity on your behalf at the end of the interview.]

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 [www.gov.uk/government/publications/cyber-security-breaches-survey].

Consent

Q1A_CONSENT
ASK IF TELEPHONE (MODETYPE = 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_VERIFYSENIOR
ASK IF WEB (MODETYPE = WEB/ONLINE)
Please could you confirm that you are a senior person responsible for cyber security in [SAMPLE S_CONAME]?

SINGLE CODE 1. Yes senior person responsible for cyber security 2. No not a senior person responsible for cyber security

SHOWSCREEN_NOTSENIOR
SHOW IF NOT A SENIOR PERSON (Q_VERIFYSENIOR CODE 2)
Thank you for your interest in this study.

Please forward the email invitation or survey link you received to the appropriate senior person in your organisation. Their feedback will shape the government's understanding of organisations like yours.
RETURN TO INTRO SCREEN

Q1X_UNICOL
ASK IF WEB OPEN LINK
Thanks for taking part via this open survey link. Ipsos is also telephoning and emailing UK further and higher education institutions directly to invite them to take part.

Just to make sure we don't call you again after you have taken part through this link, could you please provide us with the name of your institution?

WRITE IN

Incentive

Q90_DONATION
ASK IF SAMPLED AS LARGE BUSINESS (SAMPLE S_SIZEBAND=_04)
As promised, we will make a £10 charity donation on your behalf as a thank you for completing the full interview, which takes an average of 20-22 minutes. We have three charities for you to choose from.

ADD IF NECESSARY:

- Turn2us helps people in financial need gain access to charitable grants and other financial help.
- 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.

READ OUT CODES
Please select one answer

SINGLE CODE

1. Turn2us
2. NSPCC
3. Samaritans
4. DO NOT READ OUT: Prefer not to donate

Business profile

Q1B_TITLE
ASK ALL
What is your job role?

PROMPT TO CODE, INCLUDING SENIORITY AND IF RELATED DIRECTLY TO CYBER SECURITY OR NOT
Please select one answer

SINGLE CODE

Job role directly related to cyber security

1. Chief Information Officer (CIO)
2. Chief Information Security Officer (CISO)
3. Director of Security
4. Head of Cyber Security/Information Security
5. Another cyber security role

Job role directly related to IT

1. Senior IT role (e.g. IT director, Head of IT)
2. Non-senior IT role (e.g. IT manager, technician, administrator)

Job role not related to cyber security/IT - senior management level

1. Business owner
2. Chief Executive (CEO)/Managing Director (MD)
3. Chief Operations Officer (COO)/Operations Director
4. Finance Director/Controller
5. Headteacher
6. Trustee/treasurer/on trustee board
7. Partner
8. Chairperson
9. Another senior management role (e.g. director)

Job role not related to cyber security/IT - non-senior management level

1. General/office manager (not a director/trustee)
2. PA/secretary/admin
3. Teacher (not in senior management)
4. Another non-senior role

TYPEXDUM
DUMMY VARIABLE NOT ASKED
Would you classify your organisation as … ?

SINGLE CODE

1. IF SAMPLE S_SAMPTYPE=1: Private sector
2. IF SAMPLE S_SAMPTYPE=2: Charity
3. IF SAMPLE S_SAMPTYPE=3: State education institution

BUSINESS/CHARITY/EDUCATION TEXT SUBSTITUTIONS BASED ON TYPEXDUM. THIS IS THE DEFAULT SCRIPTING FOR ALL TEXT SUBSTITUTIONS FROM THIS POINT ONWARDS, UNLESS OTHERWISE SPECIFIED.

Q4_SIZEA
ASK IF BUSINESS (TYPEXDUM CODE 1)
Including yourself, how many employees work for your organisation across the UK as a whole?
This includes full-time and part-time staff. Please include yourself if you are on the payroll as an employee.
PROBE FOR BEST ESTIMATE BEFORE CODING DK

WRITE IN RANGE 2-99,999
SOFT CHECK IF >4,999

SINGLE CODE

1. Respondent is sole trader CLOSE SURVEY
2. DO NOT READ OUT: Don’t know

Q5_SIZEB
ASK IF DON’T KNOW SIZE OF BUSINESS (SIZEA CODE DK)
Which of these best represents the number of employees working for your organisation across the UK as a whole, including yourself?
PROBE FULLY
Please select one answer

SINGLE CODE

1. Under 10
2. 10 to 49
3. 50 to 249
4. 250 or more
5. DO NOT READ OUT: Don’t know

SIZEDUM
DUMMY VARIABLE NOT ASKED
Which of these best represents the number of employees working in your organisation, including yourself?

SINGLE CODE
MERGE RESPONSES FROM SIZEA AND SIZEB
USE SAMPLE S_SIZEBAND IF SIZEB CODE DK
LEAVE AS MISSING IF TYPEXDUM NOT CODE 1

1. Under 10
2. 10 to 49

3. 50 to 249
4. 250 or more

Perceived importance and preparedness

SHOWSCREEN_DISPRI
READ OUT/SHOW TO ALL
The rest of the survey is about cyber security. By this, we mean any strategy, processes, practices or technologies that organisations have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorised access.

Q9_PRIORITY
ASK IF HALF A IF BUSINESS/CHARITY, OR ALL IF EDUCATION
How high or low a priority is cyber security to your organisation's [INSERT STATEMENT]? Is it …
READ OUT STATEMENT AND SCALE
Please select one answer

ASK AS A CAROUSEL

a. [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management

SINGLE CODE
REVERSE SCALE EXCEPT FOR LAST CODE

1. Very high
2. Fairly high
3. Fairly low
4. Very low
5. DO NOT READ OUT: Don't know

Q11_UPDATE
ASK IF MEDIUM OR LARGE BUSINESSES (TYPEXDUM CODE 1 AND SIZEDUM CODES 3-4), HIGH-INCOME CHARITIES (TYPEXDUM CODE 2 AND SAMPLE S_INCOME = _04 OR _05) OR EDUCATION (TYPEXDUM CODE 3)
Approximately how often, if at all, are your organisation's [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management given an update on any actions taken around cyber security? Is it …

IF CATI AND EDUCATION (MODETYPE = CATI AND TYPEXDUM CODE 3):
INTERVIEWER NOTE: FOR EDUCATION INSTITUTIONS, "EVERY TERM" MEANS QUARTERLY
READ OUT
Please select one answer

SINGLE CODE
REVERSE SCALE EXCEPT FOR LAST 2 CODES

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

Spending

Q23X_INSUREX
ASK IF HALF A IF BUSINESS/CHARITY, OR ALL IF EDUCATION

There are general insurance policies that provide cover for cyber security breaches or attacks, among other things. There are also specific insurance policies that are solely for this purpose. Which of the following best describes your situation?
READ OUT
Please select one answer

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 breaches or attacks
4. DO NOT READ OUT: Don’t know

Information sources Q24_INFO ASK IF HALF A IF BUSINESS/CHARITY, OR ALL IF EDUCATION
In the last 12 months, from where, if anywhere, has your organisation sought information, advice or guidance on the cyber security threats that you face?
INTERVIEWER NOTE: IF “GOVERNMENT”, THEN PROBE WHERE EXACTLY
DO NOT PROMPT
PROBE FULLY, I.E. “ANYTHING ELSE?”
Please select all that apply

MULTICODE
Government/public sector

1. Government’s 10 Steps to Cyber Security guidance
2. Government’s Cyber Aware website/materials
3. Government’s Cyber Essentials materials
4. Government intelligence services (e.g. GCHQ)
5. GOV.UK/Government website (excluding NCSC website)
6. A regional Cyber Resilience Centre (CRC)

7. Action Fraud
8. National Cyber Security Centre (NCSC) website/offline
9. Police
10. Regulator (e.g. Financial Conduct Authority) but excluding charity regulators
11. Another government or public sector organisation WRITE IN

Charity-related

1. Association of Chief Executives of Voluntary Organisations (ACEVO)
2. Charity Commission/regulator
3. Charity Finance Group (CFG)
4. Community Accountants
5. Community Voluntary Services (CVS)
6. Institute of Fundraising (IOF)
7. National Council for Voluntary Organisations (NCVO)

Education related

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

Other specific organisations

1. Cyber Security Information Sharing Partnership (CISP)
2. Professional/trade/industry/volunteering association
3. Security bodies (e.g. ISF or IISP)

4. Security product vendors (e.g. AVG, Kaspersky etc)
5. UK Cyber Security Council

Internal sources

1. Within your organisation senior management/board
2. Within your organisation other colleagues or experts

Any other external sources

1. Auditors/accountants
2. Bank/business bank/bank's IT staff
3. External security/IT consultants/cyber security providers
4. Internet Service Provider
5. LinkedIn
6. Newspapers/media
7. Online searching generally/Google
8. Specialist IT blogs/forums/websites
9. Another (non-government) source WRITE IN

SINGLE CODE 40. Nowhere 41. Don't know

Q24D_SCHEME
ASK IF HALF B IF BUSINESS/CHARITY, OR IF EDUCATIONbr> There are various government campaigns, schemes, information and guidance on cyber security. Which, if any, of the following have you heard of?
READ OUT STATEMENTS
Please select one answer for each statement

IF CATI: ASK AS SEPARATE SCREENS
IF WEB: ASK AS A COLLAPSIBLE GRID

RANDOMISE LIST

a. The Cyber Essentials scheme b. The 10 Steps to Cyber Security c. IF MICRO OR SMALL BUSINESS (TYPEXDUM CODE 1 AND SIZEDUM CODES 1-2): Any Small Business Guides, such as the Small Business Guide to Cyber Security, the Small Business Guide to Response and Recovery d. IF MEDIUM OR LARGE BUSINESSES (TYPEXDUM CODE 1 AND SIZEDUM CODES 3-4), HIGH-INCOME CHARITIES (TYPEXDUM CODE 2 AND SAMPLE S_INCOME = _04 OR _05) OR EDUCATION (TYPEXDUM CODE 3): The Cyber Security Board Toolkit e. IF CHARITY: The Cyber Security Small Charity Guide f. The Cyber Aware campaign g. The “Check Your Cyber Security” tool on the National Cyber Security Centre website h. IF MICRO OR SMALL BUSINESS (TYPEXDUM CODE 1 AND SIZEDUM CODES 1-2) OR CHARITY (TYPEDUM CODE 2): The Cyber Action Plan for small organisations

SINGLE CODE

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

Q24E_GOVTACT
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND SEEN OR HEARD GOVERNMENT GUIDANCE (SCHEMEa-j CODE 1)
What, if anything, have you changed or implemented at your organisation after seeing or hearing any government campaigns or guidance on cyber security? DO NOT PROMPT
PROBE FULLY, I.E. “ANYTHING ELSE?”
Please select all that apply

MULTICODE IF CATI
Governance changes

1. Increased spending

2. Changed nature of the business/activities
3. New/updated business continuity plans
4. New/updated cyber policies
5. New checks for suppliers/contractors
6. New procurement processes, e.g. for devices/IT
7. New risk assessments
8. Increased senior management oversight/involvement

Technical changes

1. Changed/updated firewall/system configurations
2. Changed user admin/access rights
3. Increased monitoring
4. New/updated antivirus/anti-malware software
5. Other new software/tools (not antivirus/anti-malware)
6. Penetration testing

People/training changes

1. Outsourced cyber security/hired external provider
2. Recruited new staff
3. Staff training/communications
4. Vetting staff/extra vetting
5. Another change WRITE IN

SINGLE CODE

1. Nothing done
2. Only heard about guidance, not read it

3. Don’t know

Policies and procedures

SHOWSCREEN_PROCEDURES
SHOW TO ALL
Here are some questions about your current cyber security processes and procedures. If you don’t do or have the things we’re asking about, just say so and we’ll move on.

Q29_MANAGE
ASK ALL
Which of the following governance or risk management arrangements, if any, do you have in place?
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST

1. [IF BUSINESS: Board members/IF CHARITY: Trustees/IF EDUCATION: A governor or senior manager] with responsibility for cyber security
2. An outsourced provider that manages your cyber security
3. A formal policy or policies in place covering cyber security risks
4. A Business Continuity Plan that covers cyber security
5. A written list of the most critical data, systems or assets that your organisation wants to protect

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: Don’t know

2. DO NOT READ OUT: None of these

Q29A_COMPLY
ASK HALF B IF BUSINESS/CHARITY, OR ALL IF EDUCATION
Is your organisation certified with any of the following standards or accreditations?

ADD IF NECESSARY: By certified, we mean your organisation has applied for and received an optional certificate for meeting these standards or accreditations.
READ OUT
Please select all that apply

MULTICODE

1. ISO 27001
2. IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): The Cyber Essentials standard
3. IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): The Cyber Essentials Plus standard

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: Don’t know
2. DO NOT READ OUT: None of these

Q30_IDENT
ASK ALL
And which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation?
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST

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

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: Don’t know
2. DO NOT READ OUT: None of these

Q30A_AUDIT
ASK IF CARRIED OUT A CYBER SECURITY VULNERABILITY AUDIT (IDENT CODE 1)
Were any cyber security audits carried out internally by staff, by an external contractor, or both?
DO NOT PROMPT
Please select one answer

SINGLE CODE

1. Only internally by staff
2. Only by an external contractor
3. Both internal and external
4. Don’t know

Q31_RULES
ASK ALL
And which of the following rules or controls, if any, do you have in place?
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST BUT KEEP CODES 10/11 TOGETHER

1. A policy to apply software security updates within 14 days
2. Up-to-date malware protection
3. Firewalls that cover your entire IT network, as well as individual devices
4. Restricting IT admin and access rights to specific users
5. Any monitoring of user activity
6. Specific rules for storing and moving personal data files securely
7. Security controls on company-owned devices (e.g. laptops)
8. Only allowing access via company-owned devices
9. Separate WiFi networks for staff and for visitors
10. Backing up data securely via a cloud service
11. Backing up data securely via other means
12. A password policy that ensures users set strong passwords
13. A virtual private network, or VPN, for staff connecting remotely
14. An agreed process for staff to follow when they identify a fraudulent email or malicious website
15. Any requirement for two-factor authentication when people access your network, or for applications they use

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: Don’t know
2. DO NOT READ OUT: None of these

Q32_POLICY
ASK IF HAVE CYBER SECURITY POLICIES (MANAGE CODE 3)
Which of the following aspects, if any, are covered within your cyber security-related policy, or policies?
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST

1. What can be stored on removable devices (e.g. USB sticks)
2. Remote or mobile working (e.g. from home)
3. What staff are permitted to do on your organisation’s IT devices
4. Use of personally-owned devices for business activities
5. Use of cloud computing
6. Use of network-connected devices, sometimes called smart devices
7. Any Digital Service Providers such as cloud service providers, MSPs or providers of software services
8. How you’re supposed to store data

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: Don’t know
2. DO NOT READ OUT: None of these

Q63C_RANSOM
ASK HALF A IF BUSINESS/CHARITY, OR ALL IF EDUCATION

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

SINGLE CODE

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

Q33A_REVIEW
ASK IF HAVE CYBER SECURITY POLICIES (MANAGE CODE 3)
When were any of your policies or documentation for cyber security last created, updated, or reviewed to make sure they were up-to-date?

INTERVIEWER NOTE: IF NEVER UPDATED OR REVIEWED, ANSWER IS WHEN POLICIES WERE CREATED
If these policies or documentation have not yet been updated or reviewed, please tell us when they were created.
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Within the last 3 months
2. 3 to under 6 months ago
3. 6 to under 12 months ago
4. 12 to under 24 months ago
5. 24 months ago or earlier
6. DO NOT READ OUT: Don’t know

Q33B_TRAINED
ASK ALL

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

SINGLE CODE

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

Strategy

Q33D_STRATEGY
ASK IF MEDIUM OR LARGE BUSINESSES (TYPEXDUM CODE 1 AND SIZEDUM CODES 3-4), HIGH-INCOME CHARITIES (TYPEXDUM CODE 2 AND SAMPLE S_INCOME = _04 OR _05) OR FURTHER/HIGHER EDUCATION (SAMPLE S_EDUTYPE = _05 OR _06)
Does your organisation have a formal cyber security strategy, i.e. a document that underpins all your policies and processes?

SINGLE CODE

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

Q33E_STRATINT
ASK IF HAVE A CYBER SECURITY STRATEGY (STRATEGY CODE 1)
In the last 12 months, has this strategy been reviewed by your organisation’s [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management?

SINGLE CODE

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

Corporate reporting of cyber risks

Q33H_CORPORATE
ASK IF MEDIUM OR LARGE BUSINESSES (TYPEXDUM CODE 1 AND SIZEDUM CODES 3-4), HIGH-INCOME CHARITIES (TYPEXDUM CODE 2 AND SAMPLE S_INCOME = _04 OR _05) These next questions are about how cyber security is discussed in any publicly available annual reports of your organisation’s activities.

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

SINGLE CODE

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

Q33I_CORPRISK
ASK IF HAVE AN ANNUAL REPORT (CORPORATE CODE 1)
Did your latest annual report cover any cyber security risks faced by your organisation?

SINGLE CODE

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

Supplier standards

SHOWSCREEN_SUPPLYBUSINESS
SHOW IF BUSINESS (TYPEXDUM CODE 1)
The next questions are about suppliers. This is not just security or IT suppliers. It includes any suppliers that provide goods or services to your organisation.

SHOWSCREEN_SUPPLYOTHER
SHOW IF CHARITY OR EDUCATION (TYPEXDUM CODES 2-3)
The next questions are about third-party organisations you work with. This includes any suppliers that provide goods or services to your organisation, or partners such as local authorities.

Q45B_SUPPLYRISK ASK ALL
Has your organisation carried out any work to formally review the following?
READ OUT STATEMENTS
Please select one answer for each statement

IF CATI: ASK AS A GRID (NOT COLLAPSIBLE)
IF WEB: ASK AS A GRID (NOT COLLAPSIBLE)

a. The potential cyber security risks presented by your immediate suppliers [IF CHARITY/EDUCATION: or partners] b. The potential cyber security risks presented by your wider supply chain, i.e. your suppliers' suppliers

SINGLE CODE

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

Q45X_SUPPLYCERT
ASK HALF B IF BUSINESS/CHARITY, OR ALL IF EDUCATION
Do you require your suppliers to be certified with any of the following standards or accreditations?

ADD IF NECESSARY: By certified, we mean your organisation has applied for and received an optional certificate for meeting these standards or accreditations.
PROMPT TO CODE
Please select one answer for each statement

IF CATI: ASK AS A GRID (NOT COLLAPSIBLE)
IF WEB: ASK AS A GRID (NOT COLLAPSIBLE)

a. ISO 27001 b. IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): The Cyber Essentials standard c. IF HEARD OF CYBER ESSENTIALS (SCHEMEa CODE 1): The Cyber Essentials Plus standard

SINGLE CODE

1. Yes all of them
2. Yes some, but not all of them
3. DO NOT READ OUT: Don’t know
4. DO NOT READ OUT: None of these

Breaches or attacks

Q53A_TYPE
ASK ALL
Have any of the following happened to your organisation in the last 12 months, even if they ended up having no impact on you?

Please note, many of these things could happen at once or close together, i.e. as part of a related series of breaches or attacks. We want to hear about all aspects.
READ OUT
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please select all that apply

MULTICODE

1. Your organisation’s devices being targeted with ransomware, i.e. a type of malware that tells you to pay a ransom to restore your files or stop them being made public
2. Your organisation’s devices being targeted with other malware (e.g. viruses or spyware)
3. Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services
4. Hacking or attempted hacking of online bank accounts
5. People impersonating, in emails or online, your organisation or your staff [IF CHARITY: or volunteers]
6. 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
7. Unauthorised accessing of files or networks by **staff** [IF CHARITY: or **volunteers**], even if accidental
8. IF EDUCATION: Unauthorised accessing of files or networks by **students**
9. Unauthorised accessing of files or networks by people [IF BUSINESS/CHARITY: **outside your organisation**/IF EDUCATION: **other than staff or students**]
10. Unauthorised listening into video conferences or instant messaging
11. Takeovers or attempts to take over your website, social media accounts or email accounts

MULTICODE
NOT PART OF ROTATION

1. Any other types of cyber security breaches or attacks

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: Don’t know
2. DO NOT READ OUT: None of these
3. DO NOT READ OUT: Prefer not to say

Q53B_IMPERSONATIONHACK
ASK IF EXPERIENCED IMPERSONATION (TYPE CODE 5)
Just to check, did any of the instances where people impersonated your organisation or your staff involve someone gaining unauthorised access to your files or networks?
PROMPT TO CODE

SINGLE CODE

1. Yes - **all** of them
2. Yes - **some** of them
3. No
4. DO NOT READ OUT: Don’t know

Q53C_IMPERSONATIONTKVR
ASK IF EXPERIENCED IMPERSONATION (TYPE CODE 5)
And again just to check, did any of the instances where people impersonated your organisation or your staff involve someone **taking over** your own website, social media accounts or email accounts?

SINGLE CODE

1. Yes - **all** of them
2. Yes - **some** of them
3. No
4. DO NOT READ OUT: Don’t know

TYPEDUM
DUMMY VARIABLE NOT ASKED

Have any of the following happened to your organisation in the last 12 months, even if they ended up having no impact on you?

MULTICODE
MERGE RESPONSES FROM TYPE, IMPERSONATIONHACK AND IMPERSONATIONTKVR - SEE INSTRUCTIONS BELOW

1. ransomware
2. malware other than ransomware (e.g. viruses or spyware)
3. denial of service attacks
4. hacking or attempted hacking of online bank accounts
5. people impersonating, in emails or online, your organisation or your staff or volunteers
6. phishing attacks
7. unauthorised accessing of files or networks by **staff** or **volunteers**
8. unauthorised accessing of files or networks by **students**
9. IF TYPE CODE 9 OR IMPERSONATIONHACK CODES 1-2: unauthorised accessing of files or networks by people outside your organisation
10. unauthorised listening into video conferences or instant messaging
11. IF TYPE CODE 11 OR IMPERSONATIONTKVR CODES 1-2: takeovers or attempts to take over your website, social media accounts or email accounts
12. any other types of cyber security breaches or attacks
13. Don’t know
14. None of these
15. Prefer not to say

Q54_FREQ
ASK IF ANY BREACHES OR ATTACKS (TYPEDUM CODES 1-12)
Approximately, how often in the last 12 months did you experience any of the cyber security breaches or attacks you mentioned? Was it …

READ OUT
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING
REF
Please select one answer

SINGLE CODE

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

Q56A_OUTCOME
ASK IF ANY BREACHES OR ATTACKS (TYPEDUM CODES 1-12)
Thinking of all the cyber security breaches or attacks experienced in the last 12 months, which, if any, of the following happened as a result?
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST BUT KEEP CODES 3/4 AND 6/7 TOGETHER

1. Software or systems were corrupted or damaged
2. Personal data (e.g. on [IF BUSINESS: customers or staff/IF CHARITY: beneficiaries, donors, volunteers or staff/IF EDUCATION: students or staff]) was altered, destroyed or taken
3. Permanent loss of files (other than personal data)

4. Temporary loss of access to files or networks
5. Lost or stolen assets, trade secrets or intellectual property
6. Money was stolen or taken by the attackers
7. Money was paid to the attackers
8. Your website, applications or online services were taken down or made slower
9. Lost access to any third-party services you rely on
10. Physical devices or equipment were damaged or corrupted
11. Compromised accounts or systems used for illicit purposes (e.g. launching attacks)

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: None of these
2. DO NOT READ OUT: Don’t know

Q57_IMPACT
ASK IF ANY BREACHES OR ATTACKS (TYPEDUM CODES 1-12)
And have any of these breaches or attacks impacted your organisation in any of the following ways, or not?
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST BUT KEEP CODES 3/4 TOGETHER

1. Stopped staff from carrying out their day-to-day work
2. Loss of [IF BUSINESS: revenue or share value/ELSE: income]
3. Additional staff time to deal with the breach or attack, or to inform [IF BUSINESS: customers/IF CHARITY: beneficiaries/IF EDUCATION: students, parents] or stakeholders
4. Any other repair or recovery costs

5. New measures needed to prevent or protect against future breaches or attacks
6. Fines from regulators or authorities, or associated legal costs
7. Reputational damage
8. IF BUSINESS/CHARITY: Prevented provision of goods or services to [IF BUSINESS: customers/IF CHARITY: beneficiaries or service users]
9. Discouraged you from carrying out a future business activity you were intending to do
10. Complaints from [IF BUSINESS: customers/IF CHARITY: beneficiaries or stakeholders/IF EDUCATION: students or parents]
11. IF BUSINESS/CHARITY: Goodwill compensation or discounts given to customers

SINGLE CODE
NOT PART OF ROTATION

1. DO NOT READ OUT: None of these
2. DO NOT READ OUT: Don’t know

Cyber crime: cyber-facilitated fraud

SHOWSCREEN_FRAUD
SHOW IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ANY SPECIFIC BREACHES OR ATTACKS OTHER THAN IMPERSONATION (TYPEDUM CODES 1-4 OR 6-11)
The next questions focus on the following types of cyber security breaches or attacks that your organisation has experienced in the last 12 months:

SCRIPT TO SHOW ALL RESPONSES FROM TYPEDUM EXCEPT CODES 5, 12, DK, NULL AND REF - ONE RESPONSE PER LINE AND USING SHORTENED WORDING FROM TYPEDUM

IF SOME INSTANCES OF IMPERSONATION RELATED TO ANOTHER BREACH OR ATTACK, BUT NOT ALL (IMPERSONATIONHACK CODE 2 OR

IMPERSONATIONTKVR CODE 2): We know you also had instances of people impersonating your organisation or staff. Here, we only want you to include these instances if they were related to another type of breach or attack.

IF NO INSTANCES OF IMPERSONATION RELATED TO ANOTHER BREACH OR ATTACK (IMPERSONATIONHACK CODE 3 OR DK AND IMPERSONATIONTKVR CODE 3 OR DK): We know you also had instances of people impersonating your organisation or staff. You can ignore these for now.

Q88A_FRAUD
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ANY SPECIFIC BREACHES OR ATTACKS OTHER THAN IMPERSONATION (TYPEDUM CODES 1-4 OR 6-11)
How many times, if at all, did any of these cyber security breaches or attacks result in the following?
READ OUT STATEMENTS
Please write in one answer for each statement

IF CATI: ASK ON SEPARATE SCREENS
IF WEB: ASK AS A COLLAPSIBLE GRID
ROTATE LIST

a. Attackers moving money out of your organisation’s bank account b. Your organisation’s credit or debit card information being used without permission c. Your organisation paying or transferring money to the attackers based on fraudulent information (e.g. a fake invoice) d. IF ALL OR SOME INSTANCES OF IMPERSONATION RELATED TO ANOTHER BREACH OR ATTACK (IMPERSONATIONHACK CODES 1-2 OR IMPERSONATIONTKVR CODES 1-2): People impersonating your organisation or your staff using information obtained through the initial breach or attack

WRITE IN RANGE 0-99 SOFT CHECK IF>9

SINGLE CODE 1. DO NOT READ OUT: Don’t know

FRAUDDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced cyber-facilitated fraud:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF ANY FRAUDa-d>0: Yes
2. ELSE (INCLUDING IF FRAUDa-d ALL MISSING): No

FRAUDCOUNTDUM
DUMMY VARIABLE NOT ASKED
Number of cyber-facilitated fraud experienced (among those experiencing any):

IF EXPERIENCED CYBER-FACILITATED FRAUD (FRAUDDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:
FRAUDa + FRAUDb + FRAUDc + FRAUDd

ASK IF EXPERIENCED CYBER-FACILITATED FRAUD (FRAUDDUM CODE 1) AND MORE THAN ONE BREACH OR ATTACK OTHER THAN IMPERSONATION (2 OR MORE TYPEDUM CODES 1-4 OR 6-11)
The instances you just mentioned are instances of fraud.

IF FRAUDCOUNTDUM>1: Of the [FRAUDCOUNTDUM] instances of fraud your organisation experienced in the last 12 months, how many were the direct result of each of the following?
PROBE FULLY, I.E. NO NEED TO READ OUT ALL STATEMENTS IF ALL INSTANCES OF FRAUD HAVE ALREADY BEEN ACCOUNTED FOR

IF FRAUDCOUNTDUM=1: Which of the following directly resulted in this fraud?
INTERVIEWER NOTE: PUT 1 FOR "YES" AND 0 FOR "NO"
Please put 1 for "yes" and 0 for "no"

IF CATI: ASK AS A GRID (NOT COLLAPSIBLE)
IF WEB: ASK AS A GRID (NOT COLLAPSIBLE)
SCRIPT TO SHOW ONLY STATEMENTS IF EQUIVALENT STATEMENT MENTIONED AT TYPEDUM

a. Ransomware b. Malware other than ransomware (e.g. viruses or spyware) c. Denial of service attacks d. Hacking or attempted hacking of online bank accounts e. Phishing attacks f. Unauthorised accessing of files or networks by staff [IF CHARITY: or volunteers] g. Unauthorised accessing of files or networks by people outside your organisation h. Unauthorised listening into video conferences or instant messaging i. Takeovers or attempts to take over your website, social media accounts or email accounts

WRITE IN RANGE 0-[FRAUDCOUNTDUM NUMBER]
HARD CHECK IF TOTAL ACROSS ALL STATEMENTS =0

SINGLE CODE

1. DO NOT READ OUT: Don't know

FRAUDCONTDUM
DUMMY VARIABLE NOT ASKED (SEPARATE VARIABLE FOR EACH STATEMENT AT FRAUDCONT)
Cyber security breaches or attacks resulting in fraud.

IF FRAUDCONTa-i≥0: TAKE ANSWER FROM FRAUDCONT
IF EXPERIENCED CYBER-FACILITATED FRAUD (FRAUDDUM CODE 1) AND ONLY ONE BREACH OR ATTACK OTHER THAN IMPERSONATION (ONLY 1 OF

TYPEDUM CODES 1-4 OR 6-11): TAKE ANSWER FROM FRAUDCOUNTDUM AND APPLY AS FOLLOWS:

- IF TYPEDUM CODE 1: FRAUDCONTDUMa = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 2: FRAUDCONTDUMb = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 3: FRAUDCONTDUMc = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 4: FRAUDCONTDUMd = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 6: FRAUDCONTDUMe = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 7: FRAUDCONTDUMf = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 8: FRAUDCONTDUMg = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 9: FRAUDCONTDUMh = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 10: FRAUDCONTDUMi = FRAUDCOUNTDUM NUMBER
- IF TYPEDUM CODE 11: FRAUDCONTDUMj = FRAUDCOUNTDUM NUMBER

ELSE: MISSING

Q88E_FRAUDCOSTA
ASK IF EXPERIENCED CYBER-FACILITATED FRAUD (FRAUDDUM CODE 1)
IF FRAUDCOUNTDUM>1: Across these [FRAUDCOUNTDUM NUMBER] instances of fraud, what was the total cost to your organisation?

IF FRAUDCOUNTDUM=1: What was the total cost to your organisation of this fraud?

This includes:

- the direct cost of any money taken from bank accounts, credit or debit cards, or paid to the fraudsters
- other direct costs such as legal fees, insurance excess payments, or buying new software
- the cost of staff time or external contractors to help resolve or investigate issues
- the cost of any damage or disruption, such as lost revenue.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING
REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q88F_FRAUDCOSTB
ASK IF DON’T KNOW TOTAL COST OF CYBER-FACILITATED FRAUD (FRAUDCOSTA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000

8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 or more
12. DO NOT READ OUT: Don’t know

Cyber crime: ransomware

Q83X_RANSCHK
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND HAD RANSOMWARE THAT LED TO FRAUD (FRAUDCONTDUMa>0)
IF FRAUDCONTDUMa>1: Just to check, other than the [FRAUDCONTDUMa NUMBER] instances that led to fraud, did you experience any other instances in the last 12 months where **devices were targeted with ransomware**, even if the attacks were unsuccessful or did not impact your organisation?

IF FRAUDCONTDUMa=1: Just to check, other than the instance that led to fraud, did you experience any other instances in the last 12 months where **devices were targeted with ransomware**, even if the attacks were unsuccessful or did not impact your organisation?

SINGLE CODE

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

Q83E_RANSSOFT
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2)
AND
EXPERIENCED RANSOMWARE WITHOUT FRAUD (TYPEDUM CODE 1 AND FRAUDDUM NOT CODE 1) OR EXPERIENCED FRAUD THAT DIDN’T INVOLVE

THEIR RANSOMWARE (TYPEDUM CODE 1 AND FRAUDDUM CODE 1 AND (RANSCHK CODE 1 OR MISSING))
IF RANSOMWARE THAT DID NOT LEAD TO FRAUD (RANSCHK NOT CODE 1): You said you experienced at least one instance in the last 12 months where **devices were targeted with ransomware**.

Some breaches or attacks are unsuccessful, because they are stopped by an organisation's internal or third-party software before they make an impact. Others are successful, and overcome internal or third-party software.

INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

IF RANSOMWARE THAT LED TO FRAUD (RANSCHK CODE 1): Aside from [FRAUDCONTDUMa NUMBER] [instance/instances] that that led to fraud, how many, if any, of the ransomware attacks you faced in the last 12 months were successful? I.e. they overcame internal or third-party software.

IF RANSOMWARE THAT DID NOT LEAD TO FRAUD (RANSCHK NOT CODE 1): How many, if any, of the ransomware attacks you faced in the last 12 months were **successful**? I.e. they overcame internal or third-party software.

WRITE IN RANGE 0-999
SOFT CHECK IF 0: Just to check, were none of these ransomware attacks successful? I.e. were they all stopped by internal or third-party software before they made an impact?
SOFT CHECK IF>9

SINGLE CODE

1. DO NOT READ OUT: Don't know

RANSSOFTDUM
DUMMY VARIABLE NOT ASKED

Whether organisation experienced ransomware cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF RANSSOFT>0: Yes
2. ELSE (INCLUDING IF RANSSOFT MISSING): No

SHOWSCREEN_RANS
SHOW IF EXPERIENCED RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1)
IF RANSSOFT>1: This next question is specifically about these [RANSSOFT NUMBER] successful ransomware attacks you experienced [IF FRAUD (RANSCHK CODE 1):, which did not lead to fraud].
IF RANSSOFT=1: This next question is about the one successful ransomware attack you experienced [IF FRAUD (RANSCHK CODE 1):, which did not lead to fraud].

Q83H_RANSDEMA
ASK IF EXPERIENCED RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1)
IF RANSSOFT>1: Across these [RANSSOFT NUMBER] successful ransomware attacks, what was the sum total demanded in ransoms?

IF RANSSOFT=1: What was the total ransom amount demanded in this successful ransomware attack?

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

1. DO NOT READ OUT: Don’t know
2. DO NOT READ OUT: Prefer not to say

Q83I_RANSDEMB
ASK IF DON’T KNOW SUM TOTAL OF RANSOMS DEMANDED (RANSDEMA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000
8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don’t know

Q83J_RANSPAYYN
ASK IF CAN RECALL SUM TOTAL OF RANSOMS DEMANDED (RANSDEMA >1 OR RANSDEMB CODES 1-12)
And did you pay any of this amount to the attackers?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Yes, totally
2. Yes, partially
3. No
4. DO NOT READ OUT: Don’t know

Q83K_RANSPAYA
ASK IF PARTIALLY PAID RANSOM (RANSPAYYN CODE 2)
IF RANSSOFT >1: Across the [RANSSOFT NUMBER] **successful** ransomware attacks, what was the sum total you ended up paying in ransoms to the attackers?

IF RANSSOFT=1: What was the total ransom amount you ended up paying to the attackers?

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

WRITE IN RANGE £0 [RANSDEMA NUMBER OR TOP OF RANSDEMB BAND]

SINGLE CODE

1. DO NOT READ OUT: Don’t know

2. DO NOT READ OUT: Prefer not to say

Q83L_RANSPAYB
ASK IF DON'T KNOW SUM TOTAL OF RANSOMS PAID (RANSPAYA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE
ONLY SHOW CODES UNDER OR EQUAL TO ANSWER AT RANSDEMA OR RANSDEMB

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000
8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don't know

Q83M_RANSCOSTA ASK IF EXPERIENCED RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1)
IF RANSSOFT>1: Across these [RANSSOFT NUMBER] successful ransomware attacks, what was the total cost to your organisation?

IF RANSSOFT=1: What was the total cost of this successful ransomware attack to your organisation?

This includes:

- the direct cost of any ransoms paid
- other direct costs such as legal fees, insurance excess payments, or buying new software
- the cost of staff time or external contractors to help resolve or investigate issues
- the cost of any damage or disruption, such as lost revenue, or deleted files.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don't need to write the £ sign.

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

SINGLE CODE

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

Q83N_RANSCOSTB
ASK IF DON'T KNOW TOTAL COST OF RANSOMWARE CYBER CRIME (RANSCOSTA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000
8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don’t know

Cyber crime: unauthorised access

HACKDUM
DUMMY VARIABLE NOT ASKED
Number of unauthorised access events that led to fraud (used for later text substitution):

IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:
FRAUDCONTDUMf + FRAUDCONTDUMg + FRAUDCONTDUMh

Q85A_HACKCOUNT
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED UNAUTHORISED ACCESS (TYPEDUM CODES 7-10)
You said you experienced at least one instance in the last 12 months where someone

tried to access your files, networks, instant messages or conference calls without authorisation, even if they were unsuccessful or did not impact your organisation.

SCRIPT TO CHANGE INSTANCE/INSTANCES AND ATTACK/ATTACKS IN TEXT SUBS BELOW IF NUMBER>1.

IF HAD UNAUTHORISED ACCESS THAT LED TO FRAUD (HACKDUM>0) AND RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1):
Just to check, how many of these, if any, were separate from the [HACKDUM NUMBER] [instance/instances] that led to fraud, as well as the [RANSSOFT NUMBER] successful ransomware [attack/attacks] you mentioned.

IF HAD UNAUTHORISED ACCESS THAT LED TO FRAUD (HACKDUM>0) AND NO RANSOMWARE CYBER CRIME (RANSSOFTDUM NOT CODE 1):
Just to check, how many of these, if any, were separate from the [HACKDUM NUMBER] [instance/instances] that led to fraud.

IF HAD NO UNAUTHORISED ACCESS THAT LED TO FRAUD (HACKDUM NOT>0) AND RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1):
Just to check, how many of these, if any, were separate from the [RANSSOFT NUMBER] successful ransomware [attack/attacks] you mentioned.

IF HAD NO UNAUTHORISED ACCESS THAT LED TO FRAUD (HACKDUM NOT>0) AND NO RANSOMWARE CYBER CRIME (RANSSOFTDUM NOT CODE 1):
How many times did this happen?

IF HAD NO UNAUTHORISED ACCESS THAT LED TO FRAUD (HACKDUM NOT>0) AND NO SUCCESSFUL RANSOMWARE ATTACKS (RANSSOFTDUM NOT CODE 1): WRITE IN RANGE 1-999 ELSE: WRITE IN RANGE 0-999 SOFT CHECK IF>9

SINGLE CODE

1. DO NOT READ OUT: Don’t know

Q85B_HACKCOUNTDK
ASK IF DON'T KNOW HOW MANY UNAUTHORISED ACCESS EVENTS EXPERIENCED (HACKCOUNT CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. 1
2. 2 to 3
3. 4 to 5
4. 6 to 10
5. 11 to 20
6. 21 to 50
7. 51 to 100
8. More than 100
9. DO NOT READ OUT: Don't know

HACKCOUNTDUM
DUMMY VARIABLE NOT ASKED Number of instances of unauthorised access (used for later text substitution):

SINGLE CODE IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING: 1. IF HACKCOUNT>1 OR HACKCOUNTDK CODES 2-8: More than one 2. IF HACKCOUNT=1 OR HACKCOUNTDK CODE 1: One 3. ELSE: None

Q85E_HACKSIV
ASK IF ONE OR MORE UNAUTHORISED ACCESS EVENTS (HACKCOUNTDUM CODES 1-2)

Deliberate breaches or attacks are where someone knowingly gains unauthorised access. This is different to accidental breaches where, for example, an employee has accidentally accessed a file they did not have permission to use.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

IF HACKCOUNTDUM CODE 1: How many, if any, of the [HACKCOUNT NUMBER/HACKCOUNTDK CODE] instances of unauthorised access you faced were **deliberate**?

IF HACKCOUNTDUM CODE 2: Was the instance of unauthorised access you faced **deliberate**?

IF HAD UNAUTHORISED ACCESS THAT LED TO FRAUD (HACKDUM>0) OR SUCCESSFUL RANSOMWARE ATTACKS (RANSSOFTDUM CODE 1): Just as a reminder, this is separate from any instances that led to fraud, or involved ransomware.
IF HACKCOUNTDUM CODE 2: INTERVIEWER NOTE: PUT 1 FOR “YES” AND 0 FOR “NO”
IF HACKCOUNTDUM CODE 2: Please put 1 for “yes” and 0 for “no”

WRITE IN RANGE 0-[HACKCOUNT NUMBER OR TOP OF HACKCOUNTDK BAND]
SOFT CHECK IF 0: Just to check, were none of the instances of unauthorised access you faced deliberate? I.e. were they all accidental?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

HACKSIVDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced unauthorised access cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF HACKSIV>0: Yes
2. ELSE (INCLUDING IF HACKSIV MISSING): No

Q85H_HACKEXTCOUNT
SHOW IF EXPERIENCED UNAUTHORISED ACCESS CYBER CRIME (HACKSIVDUM CODE 1)
IF HACKSIV>1: How many of these [HACKSIV NUMBER] **deliberate** instances, if any, involved the attackers demanding a payment to end the unauthorised access?

IF HACKSIV=1: Did this one **deliberate** instance involve the attackers demanding a payment to end the unauthorised access?
IF HACKSIV=1: INTERVIEWER NOTE: PUT 1 FOR “YES” AND 0 FOR “NO”
IF HACKSIV=1: Please put 1 for “yes” and 0 for “no”

WRITE IN RANGE 0-[HACKSIV NUMBER]

SINGLE CODE

1. DO NOT READ OUT: Don’t know

HACKEXTDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced extortion from unauthorised access (among those experiencing any):

SINGLE CODE
IF EXPERIENCED UNAUTHORISED ACCESS CYBER CRIME (HACKSIVDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:

1. IF HACKEXTCOUNT>0: Yes
2. ELSE: No

Q85J_HACKCOSTA
ASK IF EXPERIENCED UNAUTHORISED ACCESS CYBER CRIME (HACKSIVDUM CODE 1)
IF HACKSIV>1: Across these [HACKSIV NUMBER] deliberate instances of unauthorised access, what was the total cost to your organisation?

IF HACKSIV=1: What was the total cost of this deliberate instance of unauthorised access to your organisation?

This includes:

- IF HACKEXTDUM CODE 1: any payments made to the attackers to end the attack
- any other direct costs such as legal fees, insurance excess payments, or buying new software
- the cost of staff time or external contractors to help resolve or investigate issues
- the cost of any damage or disruption, such as lost revenue, or deleted files.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

- No cost incurred

- DO NOT READ OUT: Don’t know
- DO NOT READ OUT: Prefer not to say

Q85K_HACKCOSTB
ASK IF DON’T KNOW TOTAL COST OF UNAUTHORISED ACCESS CYBER CRIME (HACKCOSTA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000
8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don’t know

Cyber crime: online takeovers

TKVRDUM
DUMMY VARIABLE NOT ASKED

Number of online takeovers that led to fraud (used for later text substitution):

IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING: FRAUDCONTDUMd + FRAUDCONTDUMi

Q86A_TKVRCOUNT

ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED ONLINE TAKEOVERS (TYPEDUM CODE 4 OR 11)

You said you experienced at least one instance in the last 12 months where someone **tried to take over your website, social media, email accounts, or online bank account**, even if they were unsuccessful or did not impact your organisation.

SCRIPT TO CHANGE INSTANCE/INSTANCES AND ATTACK/ATTACKS IN TEXT SUBS BELOW IF NUMBER>1.

IF HAD ONLINE TAKEOVERS THAT LED TO FRAUD (TKVRDUM>0) AND RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1):
Just to check, how many of these, if any, were separate from the [TKVRDUM NUMBER] [instance/instances] that led to fraud, as well as the [RANSSOFT NUMBER] successful ransomware [attack/attacks] you mentioned.

IF HAD ONLINE TAKEOVERS THAT LED TO FRAUD (TKVRDUM>0) AND NO RANSOMWARE CYBER CRIME (RANSSOFTDUM NOT CODE 1):
Just to check, how many of these, if any, were separate from the [TKVRDUM NUMBER] [instance/instances] that led to fraud.

IF HAD NO ONLINE TAKEOVERS THAT LED TO FRAUD (TKVRDUM NOT>0) AND RANSOMWARE CYBER CRIME (RANSSOFTDUM CODE 1):
Just to check, how many of these, if any, were separate from the [RANSSOFT NUMBER] successful ransomware [attack/attacks] you mentioned.

IF HAD NO ONLINE TAKEOVERS THAT LED TO FRAUD (TKVRDUM NOT>0) AND NO RANSOMWARE CYBER CRIME (RANSSOFTDUM NOT CODE 1):

How many times did this happen?

IF HAD NO ONLINE TAKEOVERS THAT LED TO FRAUD (HACKDUM NOT>0) AND NO SUCCESSFUL RANSOMWARE ATTACKS (RANSSOFTDUM NOT CODE 1): WRITE IN RANGE 1-999 ELSE: WRITE IN RANGE 0-999 SOFT CHECK IF>9

SINGLE CODE

1. DO NOT READ OUT: Don’t know

Q86B_TKVRCOUNTDK
ASK IF DON’T KNOW HOW MANY ONLINE TAKEOVERS EXPERIENCED (TKVRCOUNT CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. 1
2. 2 to 3
3. 4 to 5
4. 6 to 10
5. 11 to 20
6. 21 to 50
7. 51 to 100
8. More than 100
9. DO NOT READ OUT: Don’t know

TKVRCOUNTDUM
DUMMY VARIABLE NOT ASKED
Number of instances of online takeover (used for later text substitution):

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF TKVRCOUNT>1 OR TKVRCOUNTDK CODES 2-8: More than one
2. IF TKVRCOUNT=1 OR TKVRCOUNTDK CODE 1: One
3. ELSE: None

Q86C_TKVRSUC
ASK IF ONE OR MORE ONLINE TAKEOVERS (TKVRCOUNTDUM CODES 1-2)
IF TKVRCOUNTDUM CODE 1: How many, if any, of the [TKVRCOUNT NUMBER/TKVRCOUNTDK CODE] instances of attempted online takeover you faced were **successful**?

IF TKVRCOUNTDUM CODE 2: Was the instance of attempted online takeover you faced **successful**?

IF HAD ONLINE TAKEOVERS THAT LED TO FRAUD (TKVRDUM>0) OR SUCCESSFUL RANSOMWARE ATTACKS (RANSSOFTDUM CODE 1): Just as a reminder, this is separate from any instances that led to fraud, or involved ransomware.
IF TKVRCOUNTDUM CODE 2: INTERVIEWER NOTE: PUT 1 FOR “YES” AND 0 FOR “NO”
IF TKVRCOUNTDUM CODE 2: Please put 1 for “yes” and 0 for “no”

WRITE IN RANGE 0-[TKVRCOUNT NUMBER OR TOP OF TKVRCOUNTDK BAND]
SOFT CHECK IF 0: Just to check, were **none** of the instances of attempted online takeover you faced successful? I.e. were they all cases where someone tried and failed to gain access?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

TKVRSUCDUM
DUMMY VARIABLE NOT ASKED
Whether online takeover cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF TKVRSUC>0: Yes
2. ELSE (INCLUDING IF TKVRSUC MISSING): No

Q86H_TKVREXTCOUNT
SHOW IF EXPERIENCED ONLNE TAKEOVER CYBER CRIME (TKVRSUCDUM CODE 1)
IF TKVRSUC>1: How many of these [TKVRSUC NUMBER] **successful** online takeovers, if any, involved the attackers demanding a payment to end the takeover?

IF TKVRSUC=1: Did this one **successful** online takeover involve the attackers demanding a payment to end the takeover?
IF TKVRSUC=1: INTERVIEWER NOTE: PUT 1 FOR “YES” AND 0 FOR “NO” IF TKVRSUC=1: Please put 1 for “yes” and 0 for “no”

WRITE IN RANGE 0-[TKVRSUC NUMBER]

SINGLE CODE

1. DO NOT READ OUT: Don’t know

TKVREXTDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced extortion from online takeovers (among those experiencing any):

SINGLE CODE
IF EXPERIENCED ONLINE TAKEOVER CYBER CRIME (TKVRSUCDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:

1. IF TKVREXTCOUNT>1: Yes
2. ELSE: No

Q86J_TKVRCOSTA
ASK IF EXPERIENCED ONLINE TAKEOVER CYBER CRIME (TKVRSUCDUM CODE 1)
IF TKVRSUC>1: Across these [TKVRSUC NUMBER] **successful** online takeovers, what was the total cost to your organisation?

IF TKVRSUC=1: What was the total cost of this **successful** online takeover to your organisation?

This includes:

- IF TKVREXTDUM CODE 1: any payments made to the attackers to end the attack
- any other direct costs such as legal fees, insurance excess payments, or buying new software
- the cost of staff time or external contractors to help resolve or investigate issues
- the cost of any damage or disruption, such as lost revenue, or deleted files.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q86K_TKVRCOSTB
ASK IF DON’T KNOW TOTAL COST OF ONLINE TAKEOVER CYBER CRIME (TKVRCOSTA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000
8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don’t know

Cyber crime: hacking (dummy variables)

HACKMERGEDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced hacking cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF HACKSIVDUM CODE 1 OR TKVRSUCDUM CODE 1: Yes
2. ELSE (INCLUDING IF HACKSIVDUM OR TKVRDUM MISSING): No

HACKNUMDUM
DUMMY VARIABLE NOT ASKED
Number of hacking cyber crimes experienced (among those experiencing any):

IF EXPERIENCED HACKING CYBER CRIME (HACKMERGEDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:
HACKSIV + TKVRSUC (TREATING ANY DK VALUES AS MISSING, SO AS 0 IN THE CALCULATION)

Cyber crime: denial of service

DOSDUM
DUMMY VARIABLE NOT ASKED
Any successful and deliberate cyber security breach or attack, or cyber-facilitated fraud so far (used for later text substitution):

IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF FRAUDDUM CODE 1 OR RANSSOFTDUM CODE 1 OR HACKMERGEDUM CODE 1: Yes
2. ELSE: No

SHOWSCREEN_DOSCHK
SHOW IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED DENIAL OF SERVICE ATTACKS (TYPEDUM CODE 3) AND ANY CYBER CRIME OR CYBER-FACILITATED FRAUD SO FAR (DOSDUM CODE 1)
So far, you've told us about the following distinct cyber security breaches or attacks from the last 12 months that were both **successful and deliberate**:

SCRIPT TO CHANGE INSTANCE/INSTANCES AND ATTACK/ATTACKS IN TEXT SUBS BELOW IF NUMBER>1.

SCRIPT TO ONLY SHOW EACH BULLET BASED ON THE FOLLOWING ROUTING:

- IF FRAUDDUM CODE 1: [FRAUDCOUNTDUM NUMBER] [instance/instances] in total that led to fraud
- IF RANSSOFTDUM CODE 1: [RANSSOFT NUMBER] ransomware [attack/attacks]
- IF HACKSIVDUM CODE 1: [HACKSIV NUMBER] [instance/instances] of unauthorised access
- IF TKVRSUCDUM CODE 1: [TKVRSUC NUMBER] online takeover [attack/attacks]

This next question is specifically about any **unrelated instances** in the last 12 months where someone tried to slow or take down your website, applications or online services, known as a **denial of service attack**.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

Q87A_DOSCOUNT
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED DENIAL OF SERVICE ATTACKS (TYPEDUM CODE 3) You said you experienced at least one **denial of service attack** in the last 12 months, even if the attacks were unsuccessful or did not impact your organisation. How many times did this happen?

IF ANY CYBER CRIME OR CYBER-FACILITATED FRAUD SO FAR (DOSDUM CODE 1): Please exclude any instances related to the successful and deliberate

breaches or attacks you have already told us about. If that means you have already mentioned all your denial of service attacks, you can say this.

WRITE IN RANGE 1-999
SOFT CHECK IF>9

SINGLE CODE

1. IF DOSDUM CODE 1: DO NOT READ OUT: Already mentioned all denial of service attacks
2. DO NOT READ OUT: Don’t know

Q87B_DOSCOUNTDK
ASK IF DON’T KNOW HOW MANY DENIAL OF SERVICE ATTACKS EXPERIENCED (DOSCOUNT CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. 1
2. 2 to 3
3. 4 to 5
4. 6 to 10
5. 11 to 20
6. 21 to 50
7. 51 to 100
8. More than 100
9. DO NOT READ OUT: Don’t know

DOSCOUNTDUM
DUMMY VARIABLE NOT ASKED
Number of denial of service attacks (used for later text substitution):

SINGLE CODE

1. IF DOSCOUNT>1 OR DOSCOUNTDK CODES 2-8: More than one
2. IF DOSCOUNT=1 OR DOSCOUNTDK CODE 1: One
3. ELSE: None

Q87E_DOSSOFT
ASK IF ONE OR MORE DENIAL OF SERVICE ATTACKS (DOSCOUNTDUM CODES 1-2)
INTERVIEWER READ OUT IF NOT PREVIOUSLY MENTIONED: Some breaches or attacks are unsuccessful, because they are stopped by an organisation's internal or third-party software before they make an impact. Others are successful, and overcome internal or third-party software.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

IF DOSCOUNTDUM CODE 1: How many, if any, of the [DOSCOUNT NUMBER/DOSCOUNTDK CODE] denial of service attacks you faced were **successful**? I.e. they overcame internal or third-party software.

IF DOSCOUNTDUM CODE 2: Was the denial of service attack you faced **successful**? I.e. it overcame internal or third-party software.

IF ANY CYBER CRIME SO FAR (DOSDUM CODE 1): Just as a reminder, this is aside from the instances that led to fraud, or other successful and deliberate breaches or attacks you have already told us about.
IF DOSCOUNTDUM CODE 2: INTERVIEWER NOTE: PUT 1 FOR "YES" AND 0 FOR "NO"
IF DOSCOUNTDUM CODE 2: Please put 1 for "yes" and 0 for "no"

WRITE IN RANGE 0-[DOSCOUNT NUMBER OR TOP OF DOSCOUNTDK BAND]
SOFT CHECK IF 0: Just to check, were none of the denial of service attacks you faced successful? I.e. were they all stopped by internal or third-party software before they made an impact?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

DOSSOFTDUM

DUMMY VARIABLE NOT ASKED
Number of successful denial of service attacks (used for later text substitution):

SINGLE CODE 1. IF DOSSOFT>1: More than one 2. IF DOSSOFT=1: One 3. ELSE: None

Q87G_DOSSIV
ASK IF ONE OR MORE SUCCESSFUL DENIAL OF SERVICE ATTACKS (DOSSOFTDUM CODES 1-2)
Deliberate denial of service attacks are where someone knowingly overloads your systems to cause them to crash. This is different to non-deliberate instances where, for example, service is denied because a website is experiencing high traffic.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

IF DOSSOFTDUM CODE 1: As far as you know, how many of your [DOSSOFT NUMBER] successful denial of service attacks in the last 12 months were **deliberate**?

IF DOSSOFTDUM CODE 2: As far as you know, was your successful denial of service attacks **deliberate**?
IF DOSSOFTDUM CODE 2: INTERVIEWER NOTE: PUT 1 FOR “YES” AND 0 FOR “NO”
IF DOSSOFTDUM CODE 2: Please put 1 for “yes” and 0 for “no”

WRITE IN RANGE 0-[DOSSOFT NUMBER]
SOFT CHECK IF 0: Just to check, were **none** of your successful denial of service attacks deliberate? I.e. were they all instances of non-deliberate high traffic?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

DOSSIVDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced denial of service cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF DOSSIV>0: Yes
2. ELSE (INCLUDING IF DOSSIV MISSING): No

Q87J_DOSEXTCOUNT
SHOW IF EXPERIENCED DENIAL OF SERVICE CYBER CRIME (DOSSIVDUM CODE 1)
IF DOSSIV>1: How many of these [DOSSIV NUMBER] **successful and deliberate** denial of service attacks, if any, involved the attackers demanding a payment to end the attack?

IF DOSSIV=1: Did this one **successful and deliberate** denial of service attack involve the attackers demanding a payment to end the attack?
IF DOSSIV=1: INTERVIEWER NOTE: PUT 1 FOR “YES” AND 0 FOR “NO”
IF DOSSIV=1: Please put 1 for “yes” and 0 for “no”

WRITE IN RANGE 0-[DOSSIV NUMBER]

SINGLE CODE

1. DO NOT READ OUT: Don’t know

DOSEXTDUM DUMMY VARIABLE NOT ASKED
Whether organisation experienced extortion from denial of service attacks (among those experiencing any):

SINGLE CODE
IF EXPERIENCED DENIAL OF SERVICE CYBER CRIME (DOSSIVDUM CODE 1)
CODE AS FOLLOWS, ELSE MISSING:

1. IF DOSEXTCOUNT>0: Yes
2. ELSE: No

Q87L_DOSCOSTA
ASK IF EXPERIENCED DENIAL OF SERVICE CYBER CRIME (DOSSIVDUM CODE 1)
IF DOSSIV>1: Across these [DOSSIV NUMBER] **successful and deliberate** denial of service attacks, what was the total cost to your organisation?

IF DOSSIV=1: What was the total cost of these **successful and deliberate** denial of service attack to your organisation?

This includes:

- IF DOSEXTDUM CODE 1: any payments made to the attackers to end the attack
- any other direct costs such as legal fees, insurance excess payments, or buying new software
- the cost of staff time or external contractors to help resolve or investigate issues
- the cost of any damage or disruption, such as lost revenue, or deleted files.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q87M_DOSCOSTB
ASK IF DON’T KNOW TOTAL COST OF DENIAL OF SERVICE CYBER CRIME (DOSCOSTA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000

8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don’t know

Cyber crime: other malware

VIRUSDUM
DUMMY VARIABLE NOT ASKED
Any successful and deliberate cyber security breach or attack, or cyber-facilitated fraud so far (used for later text substitution):

IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF FRAUDDUM CODE 1 OR RANSSOFTDUM CODE 1 OR HACKMERGEDUM CODE 1 OR DOSSIVDUM CODE 1: Yes
2. ELSE: No

SHOWSCREEN_VIRUSCHK
SHOW IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED OTHER MALWARE (TYPEDUM CODE 2) AND ANY CYBER CRIME OR CYBER-FACILITATED FRAUD SO FAR (VIRUSDUM CODE 1)
So far, you’ve told us about the following distinct cyber security breaches or attacks from the last 12 months that were both **successful and deliberate**:

SCRIPT TO CHANGE INSTANCE/INSTANCES AND ATTACK/ATTACKS IN TEXT SUBS BELOW IF NUMBER>1.

SCRIPT TO ONLY SHOW EACH BULLET BASED ON THE FOLLOWING ROUTING:

- IF FRAUDDUM CODE 1: [FRAUDCOUNTDUM NUMBER] [instance/instances] in total that led to fraud
- IF RANSSOFTDUM CODE 1: [RANSSOFT NUMBER] ransomware [attack/attacks]
- IF HACKSIVDUM CODE 1: [HACKSIV NUMBER] [instance/instances] of unauthorised access
- IF TKVRSUCDUM CODE 1: [TKVRSUC NUMBER] online takeover [attack/attacks]
- IF DOSSOFTDUM CODE 1: [DOSSOFT NUMBER] denial of service [attack/attacks]

This next question is specifically about any **unrelated instances** in the last 12 months where **your organisation's devices were targeted with malware such as viruses or spyware**.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

Q84E_VIRUSSOFT
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED OTHER MALWARE (TYPEDUM CODE 2)
You said you experienced at least one instance in the last 12 months where **devices were targeted with malware such as viruses or spyware**.

INTERVIEWER READ OUT IF NOT PREVIOUSLY MENTIONED: Some breaches or attacks are unsuccessful, because they are stopped by an organisation's internal or third-party software before they make an impact. Others are successful, and overcome internal or third-party software.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

How many, if any, of the malware attacks you faced were successful? I.e. they overcame internal or third-party software.

IF ANY CYBER CRIME SO FAR (VIRUSDUM CODE 1): Just as a reminder, this is aside from the instances that led to fraud, or other successful and deliberate breaches or attacks you have already told us about.

WRITE IN RANGE 0-999
SOFT CHECK IF 0: Just to check, were none of the malware attacks you faced **successful**? I.e. were they all stopped by internal or third-party software before they made an impact?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

VIRUSSOFTDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced other malware cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF VIRUSSOFT>0: Yes
2. ELSE (INCLUDING IF VIRUSSOFT MISSING): No

SHOWSCREEN_VIRUS SHOW IF EXPERIENCED OTHER MALWARE CYBER CRIME (VIRUSSOFTDUM CODE 1) IF VIRUSSOFT>1: This next question is specifically about the [VIRUSSOFT NUMBER] **successful** malware attacks you experienced. [IF ANY CYBER CRIME SO FAR (VIRUSDUM CODE 1): These are the ones that did not lead to fraud, or involve the other successful and deliberate cyber security breaches or attacks you have already told us about].
IF VIRUSSOFT=1: This next question is about the one **successful** malware attack you experienced. [IF ANY CYBER CRIME SO FAR (VIRUSDUM CODE 1): This is the

one that did not lead to fraud, or involve the other successful and deliberate cyber security breaches or attacks you have already told us about].

Q84I_VIRUSCOSTA
ASK IF EXPERIENCED OTHER MALWARE CYBER CRIME (VIRUSSOFTDUM CODE 1)
IF VIRUSSOFT>1: Across these [VIRUSSOFT NUMBER] successful malware attacks, what was the total cost to your organisation?

IF VIRUSSOFT=1: What was the total cost of this successful malware attack to your organisation?

This includes:

- any direct costs such as legal fees, insurance excess payments, or buying new software
- the cost of staff time or external contractors to help resolve or investigate issues
- the cost of any damage or disruption, such as lost revenue, or deleted files.

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q84J_VIRUSCOSTB
ASK IF DON'T KNOW TOTAL COST OF MALWARE CYBER CRIME (VIRUSCOSTA CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £250
3. £250 to less than £500
4. £500 to less than £1,000
5. £1,000 to less than £2,000
6. £2,000 to less than £5,000
7. £5,000 to less than £10,000
8. £10,000 to less than £20,000
9. £20,000 to less than £50,000
10. £50,000 to less than £100,000
11. £100,000 to less than £250,000
12. £250,000 or more
13. DO NOT READ OUT: Don't know

Cyber crime: phishing

PHISHDUM DUMMY VARIABLE NOT ASKED
Any successful and deliberate cyber security breach or attack, or cyber-facilitated fraud so far (used for later text substitution):

IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF FRAUDDUM CODE 1 OR RANSSOFTDUM CODE 1 OR HACKMERGEDUM CODE 1 OR DOSSIVDUM CODE 1 OR VIRUSSOFTDUM CODE 1: Yes
2. ELSE: No

SHOWSCREEN_PHISHCHK
SHOW IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED OTHER MALWARE (TYPEDUM CODE 2) AND ANY CYBER CRIME OR CYBER-FACILITATED FRAUD SO FAR (PHISHDUM CODE 1)
So far, you've told us about the following distinct cyber security breaches or attacks from the last 12 months that were both **successful and deliberate**:

SCRIPT TO CHANGE INSTANCE/INSTANCES AND ATTACK/ATTACKS IN TEXT SUBS BELOW IF NUMBER>1.

SCRIPT TO ONLY SHOW EACH BULLET BASED ON THE FOLLOWING ROUTING:

- IF FRAUDDUM CODE 1: [FRAUDCOUNTDUM NUMBER] [instance/instances] in total that led to fraud
- IF RANSSOFTDUM CODE 1: [RANSSOFT NUMBER] ransomware [attack/attacks]
- IF HACKSIVDUM CODE 1: [HACKSIV NUMBER] [instance/instances] of unauthorised access
- IF TKVRSUCDUM CODE 1: [TKVRSUC NUMBER] online takeover [attack/attacks]
- IF DOSSOFTDUM CODE 1: [DOSSOFT NUMBER] denial of service [attack/attacks]
- IF VIRUSSOFTDUM CODE 1: [VIRUSSOFT NUMBER] malware [attack/attacks]

This next question is specifically about any unrelated instances in the last 12 months of **phishing attacks, where staff received a fraudulent email, or arrived at a fraudulent website**. I.e. any phishing attacks that did not lead to the instances you have already told us about. INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

Q89C_PHISHENG
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED PHISHING ATTACKS (TYPEDUM CODE 6)
You said you experienced at least one phishing attack in the last 12 months, where **staff received a fraudulent email, or arrived at a fraudulent website**.

Some phishing attacks are unsuccessful, because no one in the organisation engages with them. Others are successful, because someone engages, for example by clicking a link, opening an attachment, downloading a file, or replying to the attack email.

If more than one person engages with the same phishing attack, we want to count this as just one attack.
INTERVIEWER NOTE: PROBE IF THEY FEEL THEY UNDERSTAND BEFORE CONTINUING. REPEAT PART OR ALL OF EXPLANATION IF NECESSARY.

How many, if any, of the phishing attacks you faced did someone, such as an employee, engage with?

IF ANY CYBER CRIME SO FAR (PHISHDUM CODE 1): Just as a reminder, this is aside from the instances that led to fraud, or to other successful and deliberate breaches or attacks you have already told us about.

WRITE IN RANGE 0-999
SOFT CHECK IF 0: Just to check, did no one engage with any of the phishing attacks you faced? I.e. did no one click a link, open an attachment, download a file, or reply to the attack email?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

PHISHENGDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced phishing engagement cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF PHISHENG>0: Yes
2. ELSE (INCLUDING IF PHISHENG MISSING): No

Q89X_PHISHCONYES
ASK IF EXPERIENCED PHISHING ENGAGEMENT CYBER CRIME (PHISHENGDUM CODE 1)
Other than the [PHISHENG NUMBER] phishing [attack/attacks] that someone in your organisation engaged with, did you experience any further phishing attacks in the last 12 months?

SINGLE CODE

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

Q89E_PHISHCON ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND EXPERIENCED PHISHING ATTACKS (TYPEDUM CODE 6) WHERE NO ENGAGEMENT (PHISHCONYES CODE 1 OR PHISHENGDUM CODE 2) IF PHISHCONYES CODE 1: This question is about the remaining phishing attacks from the last 12 months that no one engaged with.

As far as you know, how many, if any, of these remaining phishing attacks were **specifically targeted** at your organisation or its staff? By this, we mean the attackers referred to your organisation or its staff by name, or included any personal or contact details in any messages.

ELSE:
And as far as you know, how many, if any, of the phishing attacks you faced in the last

12 months were **specifically targeted** at your organisation or its staff? By this, we mean the attackers referred to your organisation or its staff by name, or included any personal or contact details in any messages.

WRITE IN RANGE 0-999
SOFT CHECK IF 0: Just to check, were none of the remaining phishing attacks you faced specifically targeted at your organisation or its staff? I.e. was there no mention of your organisation, of staff by name, or other personal or contact details?

SINGLE CODE

1. DO NOT READ OUT: Don’t know

Q89F_PHISHCONDK
ASK IF DON’T KNOW HOW MANY PHISHING ATTACKS WERE TARGETED (PHISHCON CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. 1
2. 2 to 3
3. 4 to 5
4. 6 to 10
5. 11 to 20
6. 21 to 50
7. 51 to 100
8. More than 100
9. DO NOT READ OUT: Don’t know

PHISHCONDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced phishing personal details cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF PHISHCON>0 OR PHISHCONDK CODE DK: Yes
2. ELSE (INCLUDING IF PHISHCON MISSING): No

PHISHCONNUMDUM
DUMMY VARIABLE NOT ASKED
Number of phishing personal details cyber crimes experienced (among those experiencing any):

IF EXPERIENCED PHISHING PERSONAL DETAILS CYBER CRIME (PHISHCONNUMDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:
IF PHISHCON>0: TAKE VALUE FROM PHISHCON
If PHISHCONDK CODES 1-8: CODE AS FOLLOWS FROM PHISHCONDUM:

- CODE 1 = 1
- CODE 2 = 3
- CODE 3 = 5
- CODE 4 = 8
- CODE 5 = 16
- CODE 6 = 36
- CODE 7 = 76
- CODE 8 = 100

ELSE: MISSING

PHISHMERGEDUM DUMMY VARIABLE NOT ASKED
Whether organisation experienced phishing cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF PHISHENGDUM CODE 1 OR PHISHCONDUM CODE 1: Yes
2. ELSE (INCLUDING IF PHISHENG OR PHISHCON MISSING): No

PHISHNUMDUM
DUMMY VARIABLE NOT ASKED
Number of phishing cyber crimes experienced (among those experiencing any):

IF EXPERIENCED PHISHING CYBER CRIME (PHISHMERGEDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:
PHISHENG + PHISHCONNUMDUM (TREATING ANY DK VALUES AS MISSING, SO AS 0 IN THE CALCULATION)

Cyber crime (further dummy variables)

CRIMEDUM
DUMMY VARIABLE NOT ASKED
Whether organisation experienced any cyber crime:

SINGLE CODE
IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) CODE AS FOLLOWS, ELSE MISSING:

1. IF RANSSOFTDUM CODE 1 OR HACKMERGEDUM CODE 1 OR DOSSIVDUM OR VIRUSSOFTDUM CODE 1 OR PHISHMERGEDUM CODE 1: Yes
2. ELSE (INCLUDING IF ABOVE VARIABLES HAVE MISSING RESPONSES): No

CRIMENUMDUM
DUMMY VARIABLE NOT ASKED
Number of cyber crimes experienced (among those experiencing any):

IF EXPERIENCED CYBER CRIME (CRIMEDUM CODE 1) CODE AS FOLLOWS, ELSE MISSING:
RANSSOFT + HACKNUMDUM + DOSSIV + VIRUSSOFT + PHISHNUMDUM (TREATING ANY DK OR -97 VALUES AS MISSING, SO 0 IN THE CALCULATION)

Most disruptive breach or attack

SHOWSCREEN_DISRUPT
SHOW IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE TYPEDUM CODES 1-12)
Just to remind you, you mentioned that your organisation had experienced the following types of cyber security breaches or attacks in the last 12 months:

SCRIPT TO SHOW ALL MENTIONS AT TYPEDUM ONE RESPONSE PER LINE AND USING SHORTENED WORDING FROM TYPEDUM

For these final questions, we want to return to thinking about all of these.

Q64A_DISRUPTA ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND MORE THAN ONE TYPE OF BREACH OR ATTACK EXPERIENCED (2 OR MORE TYPEDUM CODES 1-12)
Now we would like you to think about the one cyber security breach or attack, or the main event in a related series of breaches or attacks, that caused the **most disruption** to your organisation in the last 12 months.

What kind of breach or attack was this?
INTERVIEWER NOTE: IF MORE THAN ONE CODE APPLIES, ASK RESPONDENT WHICH ONE OF THESE THEY THINK STARTED OFF THE BREACH OR ATTACK

PROMPT TO CODE IF NECESSARY
Please select one answer

SINGLE CODE
SCRIPT TO SHOW ONLY CODES MENTIONED AT TYPEDUM

1. Your organisation’s devices being targeted with ransomware
2. Your organisation’s devices being targeted with other malware (e.g. viruses or spyware)
3. Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services
4. Hacking or attempted hacking of online bank accounts
5. People impersonating, in emails or online, your organisation or your staff [IF CHARITY: or volunteers]
6. Phishing attacks, i.e. staff [IF CHARITY: or volunteers] receiving fraudulent emails or arriving at fraudulent websites
7. Unauthorised accessing of files or networks by **staff** [IF CHARITY: or **volunteers**], even if accidental
8. Unauthorised accessing of files or networks by **students**
9. Unauthorised accessing of files or networks by **people outside your organisation**
10. Unauthorised listening into video conferences or instant messaging
11. Takeovers or attempts to take over your website, social media accounts or email accounts
12. Any other types of cyber security breaches or attacks
13. DO NOT READ OUT: Don’t know

SHOWSCREEN_ONEATTACK
SHOW IF EXPERIENCED ONE TYPE OF BREACH OR ATTACK MORE THAN ONCE (ONLY 1 TYPEDUM CODES 1-12 AND [FREQ CODES 2-6 OR DK]): You mentioned you had experienced [INSERT SHORTENED WORDING FROM

TYPEDUM] on more than one occasion. Now I would like you to think about the one instance of this that caused the **most disruption** to your organisation in the last 12 months.

Q71_RESTORE
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
How long, if any time at all, did it take to restore business operations back to normal after the breach or attack was identified? Was it …
PROMPT TO CODE
Please select one answer

SINGLE CODE

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

Q76_REPORTA
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
Was this breach or attack reported to anyone outside your organisation, or not?

SINGLE CODE

1. Yes

2. No
3. DO NOT READ OUT: Don’t know

Q77A_NOREPORT
ASK IF MOST DISRUPTIVE BREACH OR ATTACK NOT REPORTED (REPORTA CODE 2)
What were the reasons for not reporting this breach or attack?
DO NOT PROMPT
PROBE FULLY (“ANYTHING ELSE?”)
Please select all that apply

MULTICODE

1. Breach/impact not significant enough
2. Breach was not criminal
3. Don’t know who to report to
4. No benefit to our business
5. Not obliged/required to report breaches
6. Reporting won’t make a difference
7. Too soon/haven’t had enough time
8. Worried about reputational damage
9. Another reason WRITE IN

SINGLE CODE

1. Don’t know

Q77_REPORTB
ASK IF REPORTED (REPORTA CODE 1)
Who was this breach or attack reported to?
DO NOT PROMPT

PROBE FULLY (“ANYONE ELSE?”)
Please select all that apply

MULTICODE
IT/cyber security provider

1. External IT/cyber security provider

Government or public sector organisations

1. Action Fraud
2. Cifas (the UK fraud prevention service)
3. Charity Commission/regulator
4. Information Commissioner’s Office (ICO)
5. Another regulator (e.g. Financial Conduct Authority)
6. National Cyber Security Centre (NCSC)
7. National Crime Agency (NCA)
8. National Protective Security Authority (NPSA)
9. Police
10. Another government or public sector organisation WRITE IN

Other non-government organisations

1. Antivirus company
2. Bank, building society or credit card company
3. CERT UK (the national computer emergency response team)
4. Clients/customers
5. Cyber Security Information Sharing Partnership (CISP)
6. Internet/Network Service Provider
7. Professional/trade/industry association

8. Suppliers
9. Was publicly declared
10. Website administrator
11. Another non-government organisation WRITE IN

SINGLE CODE 23. Don’t know

Q78_PREVENT
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
What, if anything, have you done since this breach or attack to prevent or protect your organisation from further breaches or attacks like this? DO NOT PROMPT
PROBE FULLY (“ANYTHING ELSE?”)
Please select all that apply

MULTICODE
Governance changes

1. Increased spending
2. Changed nature of the business/activities
3. New/updated business continuity plans
4. New/updated cyber policies
5. New checks for suppliers/contractors
6. New procurement processes, e.g. for devices/IT
7. New risk assessments
8. Increased senior management oversight/involvement
9. Purchased cyber insurance

Technical changes

1. Changed/updated firewall/system configurations
2. Changed user admin/access rights
3. Increased monitoring
4. New/updated antivirus/anti-malware software
5. Other new software/tools (not antivirus/anti-malware)
6. Penetration testing

People/training changes

1. Outsourced cyber security/hired external provider
2. Recruited new staff
3. Staff training/communications
4. Vetting staff/extra vetting
5. Another action WRITE IN

SINGLE CODE 21. Nothing done 22. Don’t know

Q78K_DAMAGEDIRS
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
These next questions are about the approximate costs of this **most disruptive** breach or attack, or related series of breaches or attacks.

Firstly, what was the approximate value of any external payments made **when the incident was being dealt with**? This includes:

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

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q78L_DAMAGEDIRSB
ASK IF DON’T KNOW SHORT-TERM DIRECT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEDIRSHO CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

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

8. £50,000 to less than £100,000
9. £100,000 to less than £500,000
10. £500,000 to less than £1 million
11. £1 million to less than £5 million
12. £5 million or more
13. DO NOT READ OUT: Don’t know

Q78M_DAMAGEDIRL
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
What was the approximate value of any external payments made **in the aftermath** of the incident? This includes:

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

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q78N_DAMAGEDIRLB
ASK IF DON’T KNOW LONG-TERM DIRECT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEDIRL CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

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

Q78O_DAMAGESTAFF
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR

BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
What was the approximate cost of the staff time dealing with the incident? This is how much staff would have got paid for the time they spent investigating or fixing the problem. Please include this cost even if this was part of this staff member's job.
PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don't need to write the £ sign.

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

SINGLE CODE

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

Q78P_DAMAGESTAFFB
ASK IF DON'T KNOW STAFF TIME COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGESTAFF CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

1. Less than £100
2. £100 to less than £500
3. £500 to less than £1,000
4. £1,000 to less than £5,000

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

Q78Q_DAMAGEIND
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ONLY ONE TYPE OF BREACH OR ATTACK EXPERIENCED OR IF CAN CONSIDER A PARTICULAR BREACH OR ATTACK (ONLY 1 TYPEDUM CODES 1-12 OR DISRUPTA NOT DK)
What was the approximate value of any damage or disruption during the incident? This includes:

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

PROBE FOR BEST ESTIMATE BEFORE CODING DK
REASSURE ABOUT CONFIDENTIALITY AND ANONYMISATION BEFORE CODING REF
Please write your answer as a whole number in £ below. You don’t need to write the £ sign.

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

SINGLE CODE

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

Q78R_DAMAGEINDB
ASK IF DON’T KNOW OTHER INDIRECT COST OF THIS CYBER SECURITY BREACH OR ATTACK (DAMAGEIND CODE DK)
Was it approximately … ?
PROMPT TO CODE
Please select one answer

SINGLE CODE

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

Incident response

Q63A_INCIDCONTENT
ASK ALL
Which of the following, if any, do you have in place, for when you experience a cyber security incident? By incident, we mean any breach or attack that requires a response from your organisation.
READ OUT
Please select all that apply

MULTICODE
ROTATE LIST

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

SINGLE CODE
6. DO NOT READ OUT: Don’t know 7. DO NOT READ OUT: None of these

Q63B_INCIDACTION ASK ALL
IF ANY BREACHES OR ATTACKS (TYPEDUM CODES 1-12): Which of the following, if any, have you done in response to any cyber security incidents you experienced in the last 12 months?
IF NO BREACHES OR ATTACKS (ELSE): Which of the following, if any, do you plan to do if you experience a cyber security incident?
READ OUT STATEMENTS
Please select one answer for each statement

IF CATI: ASK ON SEPARATE SCREENS
IF WEB: ASK AS A COLLAPSIBLE GRID
RANDOMISE LIST

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

SINGLE CODE

1. Yes
2. No
3. DO NOT READ OUT: Don’t know
4. DO NOT READ OUT: Depends on/did not reflect the severity or nature of the incident

Recontact and follow-up

Q78K_VALIDATE
ASK IF TELEPHONE (MODETYPE = CATI)
ASK IF BUSINESS/CHARITY (TYPEXDUM CODES 1-2) AND ANY BREACHES OR ATTACKS (TYPEDUM CODES 1-12) AND DID NOT ANSWER “PREFER NOT TO SAY” TO ALL COST QUESTIONS (NOT DAMAGEDIRS, DAMAGEDIRL, DAMAGESTAFF, DAMAGEIND ALL REF)
We’d like to send you a quick email afterwards giving you the chance to validate the answers for the questions about the number and cost of different breaches or attacks. It really helps to ensure we can properly report the impact of these kinds of cyber attacks.

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

Are you happy for us to email you?

SINGLE CODE

1. Yes
2. No

Q79_RECON
ASK ALL
Ipsos expects to undertake further research on the topic of cyber security within the next 12 months. In these research studies, we would again randomly sample businesses in your industry sector and your business may be selected. In this case, having your individual contact details would save us from having to contact your switchboard, or email another part of your business.

With this in mind, would you be happy for us to securely hold your individual contact details for this purpose for the next 12 months?

SINGLE CODE

1. Yes
2. No

Q80_REPORT
ASK IF WEB (MODETYPE = WEB/ONLINE)
OR
ASK IF TELEPHONE (MODETYPE = CATI) AND ANSWER “PREFER NOT TO SAY” TO ALL COST QUESTIONS (DAMAGEDIRS, DAMAGEDIRL, DAMAGESTAFF, DAMAGEIND ALL REF) Would you like us to email you a copy of last year’s report and a Government help card, with links to the latest official cyber security guidance for organisations like yours?

SINGLE CODE

1. Yes

2. No

Q81_EMAIL
ASK IF WANT VALIDATION SURVEY (VALIDATE CODE 1) RECONTACT (RECON CODE 1) OR REPORT/HELPCARD (REPORT CODE 1)
Can we please take your contact details, so we can contact you only for the agreed reasons?
PROMPT TO CODE

SCRIPT TO COLLECT CONTACT NAME, CONTACT JOB TITLE, VALID EMAIL AND VALID TELEPHONE IN 4 SEPARATE BOXES 1. Prefer not to say

SEND WEB INVITE IF VALIDATE CODE 1 SEND FOLLOW-UP EMAIL IF REPORT CODE 1

SHOWSCREEN_END SHOW TO ALL Thank you for taking the time to participate in this study. You can access the privacy notice online at [www.gov.uk/government/publications/cyber-security-breaches-survey]. This explains the purposes for processing your personal data, as well as your rights under data protection regulations to:

- access your personal data
- withdraw consent
- object to processing of your personal data
- and other required information.

CLOSE SURVEY

Web follow-up

SHOWSCREEN_VALIDATE
SHOW IF ELIGIBLE FOR WEB SURVEY (VALIDATE CODE 1)

Thanks for taking part. The next screens give you the chance to recheck or correct any cost information you gave us in the telephone survey.

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

Q82_CHECKA
ASK IF ANSWERED ONE OF THE DISRUPTIVE BREACH COST QUESTIONS ((DAMAGEDIRSB NOT DK AND DAMAGEDIRS NOT REF OR NULL) OR (DAMAGEDIRLB NOT DK AND DAMAGEDIRL NOT REF OR NULL) OR (DAMAGESTAFFB NOT DK AND DAMAGESTAFF NOT REF OR NULL) OR (DAMAGEINDB NOT DK AND DAMAGEIND NOT REF OR NULL)) You said the most disruptive cyber security breach or attack you had in the last 12 months was: [ANSWER AT DISRUPTA].

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

ASK AS A COLLAPSIBLE GRID

● IF DAMAGEDIRSB NOT DK: You said the approximate value of any external payments made **when the incident was being dealt with was [ANSWER AT DAMAGEDIRS OR DAMAGEDIRSB]**. This includes:

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

a. IF DAMAGEDIRLB NOT DK: You said the approximate value of any external payments made in the aftermath of the incident was **[ANSWER AT DAMAGEDIRL OR DAMAGEDIRLB]**. This includes:

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

b. IF DAMAGESTAFFB NOT DK: You said the approximate cost of the staff time dealing with the incident was **[ANSWER AT DAMAGESTAFF OR DAMAGESTAFFB]**. This is how much staff would have got paid for the time they spent investigating or fixing the problem. Please include this cost even if this was part of this staff member's job.

c. IF DAMAGEINDB NOT DK: You said the approximate value of any damage or disruption during the incident was [ANSWER AT DAMAGEIND OR DAMAGEINDB]. This includes:

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

SINGLE CODE

1. Correct
2. Incorrect

SHOWSCREEN_VALIDATEEND
SHOW IF ELIGIBLE FOR WEB SURVEY (VALIDATE CODE 1)
Thank you for taking the time to participate in this study. You can access the privacy notice online at [www.gov.uk/government/publications/cyber-security-breaches-survey]. 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

Cyber Security Breaches Survey 2024 Qualitative topic guide

Structure of the topic guide (for interviewers)	Timings
Introduction	2-3 minutes
Perception of cyber security risk	2-3 minutes
Impact of economic uncertainty	10 minutes
Cyber security leadership and governance	20 minutes

Incident response	Corporate annual reporting on digital strategy and risks	Digital Service Providers	10 minutes
Standards and accreditation decision-making	Supply chain decisions		5 minutes
Summary and wrap-up			5 minutes

Introduction (FOR ALL)	**2-3 minutes**
● Thank participant for taking part; introduce self and Ipsos ● Explain the project: we are exploring some topics about cyber security from the survey in more depth on behalf of DSIT and the Home Office ● All responses are confidential and anonymous ● £50 thank you for taking part (voucher or charity donation) ● Recording: get permission to digitally record ● Length: approximately 60 mins **GDPR added consent (once the 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 January 2024.	Welcomes and prepares the participant. Informs them about key aspects of the interview, including those we are required to include under MRS guidelines and GDPR. (Make this brief: these participants took part in the quantitative survey and should understand the background.)

Can I check that you are happy to proceed?

Perception of cyber security risk (ASK ALL)	**2-3 minutes**
SKIP IF THEY ARE PRESSED FOR TIME ● Briefly, what would you say are the top 2-3 cyber security priorities for your organisation right now?	Icebreaker section with easy open questioning. Gains initial overview of cyber security priorities.
Impact of economic uncertainty	10 minutes
● How has awareness of cyber resilience and cyber risks (e.g. cyber espionage, IP theft, data breaches, hacks and leaks, impact on reputation) changed over the last 12 months? o What prompted these changes, if any? o What impact have these changes had, if any? o Have current economic conditions had an impact on your awareness of or attitudes towards cyber resilience and cyber risks? Have they impacted on your ability to implement tools / software that will spot cyber security breaches? o Has this changed over the last 12 months? ● Overall, how has your investment in cyber security changed over the last few years? Has it trended upwards/downwards? What has driven this? ● How do you see cyber resilience and cyber risks	

changing over the next 12 months?

o How do you see your investment changing over the next 12 months?
o Why do you say that?

Cyber security leadership and governance - part A (ASK ALL)	**20 minutes**

<u>Developing and implementing cyber security strategy</u>

● Can you briefly summarise your organisation's overarching approach to cyber security? Why do you take this approach?

o How do you formalise this approach, if at all?
o How does the board monitor and update your approach to cyber security?
o IF HAVE CYBER SECURITY STRATEGY AT Q33D: What is contained in your cyber security strategy?
o Who has responsibility for it (PROBE ON BOARD)? How is it updated?
o And what current guidance do you use to help develop and implement your cyber security strategy?

● IF SMALL OR MEDIUM ORGANISATION: NCSC have recently launched the Cyber Advisor scheme, which offers practical hands-on-help for smaller organisations through a network of NCSC Assured Advisors. Are you aware of this scheme?

This section seeks to understand decision-making around cyber security, and which staff are involved.

There is around 8-10 minutes each on the 2 big topics (budget and board), then potentially a few mins on culture/ behaviour change.

Ideally get participants to share their screen when looking at the Board Toolkit, so we can see the bits they provide feedback on.

The section on board engagement may turn out to be less relevant for smaller businesses (e.g. where we are already talking to a founder). Use your judgement to decide whether to ask this subsection

o IF AWARE: Have you used Cyber Advisor scheme? IF YES: How did you find it? What do you think could have been improved? IF NO: Why not? What did / didn't you think you could get out of it?
o IF NOT: Would a service like this for smaller organisations be useful to you?
o IF MEDIUM OR LARGE ORGANISATION: NCSC have recently revised the Cyber Security Board Toolkit. Have you used the Board Toolkit this year? IF YES: And did you find it useful?

● IF ANSWERED THAT CYBER SECURITY IS A LOW PRIORITY: You said in the previous interview that cyber security wasn't a high priority for your organisation. Are you able to go into a bit more detail about this and why it isn't currently a high priority?

Roles and responsibilities

PRIORITY: The next few questions are about roles and responsibilities of board members

● How closely are board members (directors, trustees etc.) and your executive team (CEOs etc.) involved in cyber security decisions? PROBE INVOLVEMENT IN:

o Deciding what your cyber security priorities/critical assets are
o Spending decisions (including staffing and outsourcing)

or skip it (and spend more time on culture change or information seeking).

If we interview schools/ colleges, we'll refer to the Senior Leadership Team instead of the board/executive team.

o Incident response

● How frequently is cyber security discussed at the Board or at senior management meetings (e.g. ad hoc, standing agenda item)?

● Do you receive any support or advice from external experts around cyber security? If so, from who (e.g. outsourced providers, auditors)? Why do you need to use these?

● How would you describe board members' understanding of cyber security issues and reports?

IF TIME: The next few questions are about roles and responsibilities of the wider team

● Who is responsible in your organisation for managing and protecting key digital assets and data?

● Who is responsible for cyber security and how do they report to the board?

Embedding cyber security in risk management

● How well are your organisation's cyber security needs understood by …

o Members of the Board (IF RELEVANT)
o Members of the executive team

● How well do they understand your approach? PROBE:

o What bits do they understand well/less well? What further support would you want to see from them on cyber security?
o How do cyber security risks fit into wider risk management?
o How frequently do you assess the threat environment, technology developments and your capabilities?

Incident planning

● How prepared would you say your wider staff are for a major cyber attack or cyber incident, if it took place tomorrow?

● You mentioned in the survey that you have plans in place if you experience a cyber security incident [SEE SURVEY RESPONSE AT Q63A/B].

o What types of cyber security incidents does this cover?
o How do you go about preparing against cyber security incidents?
o Who is responsible for signing these off? What guidance or advice do you receive on this, and from whom?

● What's the biggest challenge in this planning for incidents? What do you find hard? PROBE:

o Willingness/pushback from staff
o Skills of staff/senior management
o Time/capacity of staff
o Hybrid working
o Budgets/training budgets

Incident response (ON ROTATION, LISTED IN THE SAMPLE PROFILE)	**10 minutes**
[SEE SURVEY RESPONSES TO Q63A / Q63B FOR CONTEXT AND REPHRASE QUESTIONS ACCORDINGLY] We'd now like to move away from incident planning and ask you about incident response in the aftermath of a breach. ● **What is the first thing you would do when you notice any suspicious activity?** ● **How do you assess the severity / potential impact of an incident or breach?** ● **Would you be able to briefly walk us through the journey of how you typically respond to an impactful breach?** o In the survey you said you [SEE SURVEY RESPONSES TO Q63A / Q63B] in response to a breach. Is this consistent across all breaches? What drives you to take action? What other actions do you take? o How has your actual response to a severe breach	This is trying to understand why organisations do and don't report breaches, the circumstances that lead them to report, and their knowledge around reporting. The NCSC encourages all organisations to report phishing emails, scam websites, phone calls and adverts. It does not deal with cybercrime, which it says should be reported to Action Fraud or Police Scotland.

differed to what was planned? How did this impact overall response? IF TALKING ABOUT RANSOMWARE: Did it involve making payments?
o What do you do once the breach has been contained? Why is this?
o In what stage and type of incident would you involve the Board or senior management?

● Under what circumstances would you not report a cyber security incident or breach? Why not?

● Do you have a policy or rules around post-incident reviews with the board and management?

● How do you think your approach to incident response can be improved? What kind of support would you need in helping to address this?

● What types of cyber security incident would lead to you alerting any of the following bodies or groups:

o A regulator
o Your bank or insurance company
o The police or a related body like Action Fraud what kinds of breaches do you think they are interested in hearing about? Had you heard of Action Fraud before (https://www.actionfraud.police.uk/)?
o The National Cyber Security Centre what kinds of

breaches do you think they are interested in hearing about?
o Your customers, investors or suppliers

● Do you think other organisations in your sector take the same approach?

● Have you previously reported breaches to any of the bodies or groups mentioned above?

o IF YES: Please talk me through the breach and the decision behind reporting it.
o What were the advantages and disadvantages of reporting?
o How did you decide who to report the breach to? Did you receive any third party advice on actions to take?
o IF NOT REPORTED A BREACH: Please talk me through what informed this decision (e.g. cost / benefit, third party influence).

● Have you ever had a serious breach you didn't report to anyone externally? IF YES: Please talk me through the breach and why you didn't report it.

Corporate annual reporting on digital strategy and risks (ON ROTATION, LISTED IN THE SAMPLE PROFILE)	**10 minutes**
In the survey you said that your organisation included a section on your digital strategy and risks in your last annual report.	This section explores the inclusion of cyber security content in annual reports.

● What is the main purpose of this section? Who is the intended audience?

● Could you outline the content of this section? What information was included? PROBE:

o Digital or cyber strategy, risk assessments, governance arrangements, technical settings, training, supply chains, incidents
o Would you typically exclude any of these areas? What's the rationale behind that?

● How is this section compiled and edited? PROBE:

o Who writes it? Who decides on content and focus? Who approves it?
o How much involvement does the board/executive team have over this section of the report? How much is left to the cyber/IT team alone?

Digital Service Providers (ON ROTATION, LISTED IN THE SAMPLE PROFILE)	**10 minutes**
This section is about Digital Service Providers, or DSPs, that manage a suite of IT services like your network, cloud computing and applications. In the survey, you said your organisation used one or more DSPs. This may include Managed Service Providers (MSPs). ● What do(es) your DSP(s) provide? Is it a	This section explores DSPs, which are a potential source of risk on cyber security if poorly chosen. This looks at how organisations choose DSPs and manage their relationships with them.

software package or a service? How essential are they to your continuity of production/service? ● What were the factors involved in choosing your DSP(s)? o Was cyber security one of the considerations? IF YES: How much of a priority would you say this was compared to other factors (e.g. price, reliability, word of mouth)? ● How much of a risk do you think your DSP(s) poses to your organisation's cyber security? o Have you discussed this with them? How willing are they to discuss it/share information on their cyber security? o Does your contract with your DSP say anything about cyber security? What's covered? ● Who is responsible for cyber security between them and you, when it comes to their service? E.g. for incident response?	
Cyber security practices	**5 minutes**
<u>Privacy enhancing technologies</u> ● Do you currently use any privacy enhancing technologies as part of your approach to cyber security? o If so, what kinds of privacy enhancing	Accreditations might include ISO 27001, Cyber Essentials, Cyber Essentials Plus - these are the ones we cover in the survey. The NCSC Cyber Assessment

technologies do you use?
o And how are these technologies used to protect customers?

Standards and accreditation decisions (IF HAVE ACCREDITATIONS)

● Tell us about the external cyber security standards and accreditations your organisation has adopted.

o What made you decide to apply for this? PROBE: internal pressure (e.g. board members), external pressure/requirements from clients, investors, insurance providers, for branding/marketing, etc.
o What made you choose this standard over others? PROBE: ISO 27001, Cyber Essentials, Cyber Essentials Plus, NIST
o What involvement did your board/executive team have in this? How well do they understand this standard and what it means?
o How has this standard improved your cyber security? What changes did you have to make to meet this standard, if any?

● Have your cyber security standards and accreditations helped you win contracts or new business?

● Have you heard of the NCSC's Cyber Assessment Framework? Have you used this in your organisation? What has your experience been?

Framework was primarily designed for Critical National Infrastructure organisations, but can also be used by other large businesses.

ICO

● Are your cyber security measures impacted by the rules and regulations set out by the Information Commissioner's Office?

Supply chain decisions (IF HAVE SUPPLY CHAIN MANAGEMENT)

● How do you go about managing cyber security risks from your wider supply chains? How systematic/formalised is this process?

o Do you use software for this?
o Does your organisation use Cyber Essentials as a means of managing the cyber security risks from your wider supply chains? Do you take it into account when choosing suppliers, or recommend it to or require it of suppliers?

● Who is responsible? How engaged are your board/executive team in this?

● How would you describe your awareness/monitoring of the risks? PROBE: Do you know which suppliers have access to your IT systems? Which ones are essential to your continuity of production/service?

● How do you seek assurance from suppliers of different risks? PROBE: Do you want more assurance from critical suppliers and less from

others?

● How often do you talk to your suppliers about cyber security? How do you ensure they are aware of their responsibilities?

o When do you talk to suppliers about cyber security, do you ask them if they use ‘secure by design’ principles in their software design?

● How would you react to suppliers if they had cyber security incidents affecting you? Would you expect to provide any support?

● Do you supply to other businesses or organisations?

o IF PARTICIPANT IS A SUPPLIER: Do you know your cyber security contractual obligations as a supplier?

o What do you have to report to your client businesses? How do you monitor and evidence this?

o If you experienced a cyber security incident, how would this impact the businesses / organisations that you supply? Would you expect to receive any support?

● Has anything changed in terms of how you look at cyber security risks from your supply chains in the last 2 years? Has it got any more/less important?

● Is there more you would want to do about assessing or monitoring supply chains? What are the barriers to doing this?	
Summary & wrap-up	**Do at/just after the hour mark**
● Thinking about all the challenges we talked about, are there any areas that you think your organisation could improve on, or could focus on more? ● What's the most important thing you think we have talked about? ● Would you be willing to take part in any further interviews with DSIT or the Home Office in the next 12 months?	An opportunity for final reflections. We also want to maintain permission to recontact for where possible.

Appendix C: Further information

1. The Department for Science, Innovation and Technology and the Home Office would like to thank the following people for their work in the development and carrying out of the survey and for their work compiling this report.

- Alice Stratton, Ipsos
- Nada El-Hammamy, Ipsos
- Sally-Ann Barber, Ipsos
- Finlay Proctor, Ipsos

- Nick Coleman, Ipsos
- Jayesh Navin Shah, Ipsos.

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

3.The lead DSIT analyst for this release is Maddy Ell. The responsible statistician is Saman Rizvi. For enquiries on this release, from an official statistics perspective, please contact DSIT at cybersurveys@dsit.gov.uk.

4.The Cyber Security Breaches Survey is an official statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https:/code.statisticsauthority.gov.uk/. Details of the pre-release access arrangements for this dataset have been published alongside this release.

5.This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252.

---

1. See https://www.gov.uk/government/publications/information-security-breaches-survey-2015 (https://www.gov.uk/government/publications/information-security-breaches-survey-2015) for the final survey in this series. This was preceded by earlier surveys in 2014, 2013 and 2012. We reiterate that these surveys are not representative of all UK businesses and are not comparable to the Cyber Security Breaches Survey series.
2. These are organisations that work for a social purpose, but are not registered as charities, so are not regulated by the UK's charity regulators.

3. SIC sectors here and in subsequent tables in this report have been combined into the sector groupings used in the main report.
4. This excludes the two weeks around the Christmas and New Year bank holidays, during which there was minimal fieldwork conducted.
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 (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 (availble at: https://academic.oup.com/poq/issue/81/2 (https://academic.oup.com/poq/issue/81/2).
6. The default SPSS setting is to round cell counts and then calculate percentages based on integers.

↑ Back to top