Department for
Science, Innovation
& Technology

Official Statistics

Cyber security breaches survey 2025/2026

Published 30 April 2026

Contents

This publication is available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026

The Cyber Security Breaches Survey is a research study on UK cyber resilience. 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 and qualitative interviews were carried out between August and December 2025.

Lead analyst:

Emma Johns (DSIT)

Responsible statisticians:

Saman Rizvi (DSIT)

Lamyr Megnin (Home Office)

Enquiries:

cybersurveys@dsit.gov.uk

Summary

Introduction

The Cyber Security Breaches Survey 2025/2026, was commissioned by the Department for Science, Innovation and Technology (DSIT) and the Home Office. It provides a comprehensive overview of the cyber security landscape for UK businesses and charities. Results for public sector schools, colleges and universities are covered in the separately published Education annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings).

This report summarises key findings from the survey, highlighting trends in cyber security awareness, approaches to risk management, prevalence and impact of breaches, incident response, and the evolving threat of cyber crime.

This publication is accompanied by data tables containing most of the questions asked in the survey (excluding questions related to cyber crime), broken down by organisation type, business size, and charity income band.

Identification of cyber security breaches and attacks

The survey only includes the breaches or attacks that organisations were able to identify and willing to report. There are likely to be hidden attacks, and other breaches that go unidentified, so the findings reported here may underestimate the full extent of the prevalence of cyber breaches and attacks.

Just over four in ten businesses (43%) and around three in ten charities (28%) reported having experienced any kind of cyber security breach or attack in the last 12 months. This equates to approximately 612,000 UK businesses and 57,000 UK charities[footnote 1]. Overall prevalence of cyber breaches or attacks has remained in line with last year, after a significant decline in prevalence among businesses the previous year (from 50% in 2023/2024 to 43% in 2024/2025).

Following the pattern observed in previous years, medium (65%) and large (69%) businesses were more likely to have experienced a cyber breach or attack in the last 12 months compared to micro (42%) and small (46%) businesses.

It should be noted that cyber security breaches and attacks are different from cyber crimes (under the Computer Misuse Act 1990 and the Home Office Counting Rules). Cyber crimes are a subset of cyber breaches and attacks and should be considered as a distinct set of figures that are referred to later in the report.

Phishing attacks remained the most prevalent type of breach or attack by far (experienced by 38% of businesses and 25% of charities) and continued to be ascribed as the most disruptive type of breach or attack (69% of businesses and charities that experienced a breach or attack). Among those who experienced a breach or attack, the proportion experiencing phishing attacks only (and no other type of breach or attack) has increased among both businesses (from 45% last year to 51% this year) and charities (from 46% last year to 57% this year). The qualitative interviews highlighted interviewees' perception that phishing attacks had become easier for attackers to commit, and that this was contributing to what they perceived as an increase in attack volumes.

Ransomware attacks among businesses have declined compared with the previous two years (1% this year down from 3% in both 2024/2025 and 2023/2024) and phishing attacks and impersonation breaches or attacks,

whilst not significantly different to last year, have significantly declined compared to two years ago (38% this year down from 42% in 2023/2024). Impersonation breaches or attacks have decreased to 12% this year, down from 17% in 2023.

Among charities there have been significant decreases in the proportion of charities experiencing impersonation breaches or attacks and experiencing a takeover. Impersonation breaches or attacks were significantly down compared with the previous two years (7% this year down from 11% in 2024/2025 and 12% in 2023/2024). The proportion of charities experiencing a takeover has decreased from 3% in 2024/2025 to 1% this year (although was in line with 2% in 2023/2024).

The proportion of businesses and charities experiencing any negative outcome following a breach or attack has remained consistent with 2024/2025 (19% for business and 11% for charities in 2025 compared to 16% for both businesses and charities in 2024/2025). However, there has been an increase in businesses reporting that the breach or attack led to loss of revenue or share value (2% in 2024/2025 to 5% in 2025/2026) and an increase in those reporting it resulted in reputational damage (1% in 2024/2025 to 3% in 2025/2026).

The median perceived cost of the most disruptive breach or attack was £0 for businesses and £0 for charities, increasing to £30 for medium and large businesses. The range of perceived cost where most fell (25th to 75th percentile) was £0 to £200 for businesses and £0 to £80 for charities, suggesting that the majority of businesses did not experience high costs for their most disruptive breach or attack. Looking at the perceived cost for the top 5% of cases (95th percentile), however, does show that in a minority of cases organisations can face high costs (£4,000 for all businesses and micro/small businesses, rising to £10,000 for medium/large businesses, and £1,000 for charities). Perceived costs were higher when an outcome from the breach or attack was experienced or when just those who had a material financial cost (not £0) were included.

Cyber hygiene

Cyber hygiene refers to the cyber security practices of organisations, including their risk management, technical controls, and cyber governance.

The majority of businesses and charities have implemented basic technical controls, such as updated malware protection (81% businesses and 63% charities), backing up data securely via a cloud service (74% businesses and 57% charities), password policies (74% businesses and 56% charities), network firewalls (74% businesses and 45% charities) and restricted admin rights (73% businesses and 65% charities). However, adoption of more

advanced controls like two-factor authentication (47% businesses and 38% charities), a virtual private network for staff connecting remotely (36% businesses and 17% charities) and user monitoring (30% businesses and 31% charities) remain lower than other measures.

Micro businesses saw some uplifts in the deployment of controls and procedures, including increases in those that only allow access via company-owned devices (64% up from 58% in 2024/2025), and those that require two-factor authentication (43% up from 35% in 2024/2025). The proportion of micro businesses with an external cyber security provider also increased (44% up from 39% in 2024/2025).

However, despite improvements in several cyber hygiene practices last year, small businesses saw a return to 2023/2024 levels, including undertaking cyber security risk assessments (41%, a decrease from 48% in 2024/2025), having a formal cyber security policy covering cyber security risks (52% down from 59% in 2024/2025), and business continuity plans that address cyber security (44% down from 53% in 2024/2025).

A formal cyber security strategy was in place for almost six in ten medium businesses (57%), rising to seven in ten large businesses.

Around one in seven businesses (14%) and one in five charities (22%) said they held personal data that was not protected by techniques such as anonymisation or encryption, suggesting that the majority do protect personal data (77% of businesses and 69% of charities).

Qualitative insights highlighted that recent high-profile cyber attacks in the media had moved the perception risk from cyber attacks and breaches up the agenda within organisations. Despite this, staff training and awareness raising activities remained stable across businesses compared with last year (19% in both 2024/2025 and 2025/2026). There were signs of an increase among large businesses (76% in 2024/2025 to 84% in 2025/2026) but this did not represent a significant change. On the other hand, the proportion of charities running staff training and awareness raising activities has decreased since last year (17% in 2025/2026, down from 21% in 2024/2025), driven by a decline among low-income charities (13% in 2025/2026, down from 18% in 2024/2025).

Risk management

Around a third of businesses (30%) conducted a risk assessment covering cyber security, in line with last year (29%). The same was true for charities (27%, in line with 29% last year).

When it came to supply chains, relatively few businesses or charities were taking steps to formally review the risks posed by their immediate suppliers and wider supply chain. Just over one in ten businesses said they reviewed the risks posed by their immediate suppliers (15%) and under one in ten were looking at their wider supply chain (6%). Among charities, the respective figures were slightly lower (9% looked at their immediate suppliers and 4% at their wider supply chain). This varied by size, possibly reflecting a more complex supply chain among medium and large businesses, with around a third of medium businesses (30%) and nearly half of large businesses (48%) reviewing the cyber security risks posed by their immediate suppliers, in comparison to 12% of micro businesses and 22% of small businesses.

Almost half of businesses (47%) and a third of charities (35%) reported being insured against cyber security risks in some way. As in previous years, small (55%) and medium (61%) businesses were more likely than businesses overall (47%) to have some form of cyber insurance.

Around a third of businesses (31%) and a quarter of charities (25%) were either using AI, in the process of adopting it or actively considering using it. Of this group, around a quarter of businesses (24%) and charities (27%) reported having cyber security practices or processes in place to manage the risks from the use of AI technology.

Board engagement and corporate governance

Cyber security was considered a high priority for senior management in around seven in ten businesses (72%) and six in ten charities (60%). While this was broadly consistent with recent years for businesses, charities saw a significant decline compared with 2024/2025 (down from 68% to 60%), driven by low-income charities. Board-level responsibility for cyber security sat at 31% of businesses and 30% of charities and continued to be higher in larger businesses (68% of large businesses). Compared with 2024/2025, the proportion of businesses with board level responsibility for cyber security increased (from 27%), reversing the longer-term downward pattern seen earlier in the decade.

Cyber accreditations and following guidance

Seeking external information or guidance on cyber security was reported by 44% of businesses and 31% of charities. For charities, this aligns with the wider picture this year of reduced prioritisation of cyber security, and reflects a decrease compared with 2024/2025.

The most commonly cited individual source of information remained external cyber security or IT consultants/providers (27% of businesses and 13% of charities). As in previous years, relatively few organisations named specific official bodies as sources of advice: 1% of businesses and 1% of charities mentioned the National Cyber Security Centre (NCSC) by name.

When prompted about government initiatives, recognition was higher and increased compared with 2024/2025, reversing a longer-term decline. Cyber Aware was recognised by 30% of businesses and 30% of charities, while awareness of the Software Security Code of Practice was 22% for businesses and 19% for charities, awareness of the 10 Steps guidance was 17% for businesses and 19% for charities, awareness of Cyber Essentials was 17% for businesses and 16% for charities, and awareness of the Cyber Governance Code of Practice was 16% for both businesses and charities.

Despite relatively low prompted awareness overall, a larger share of organisations reported having the technical controls associated with Cyber Essentials (24% of businesses and 13% of charities reported controls in all five areas).

The proportion of businesses holding Cyber Essentials has increased since 2024/2025 (5% up from 3% in 2024/2025). This was driven by increases among large businesses (from 21% in 2024/2025 to 35% in 2025/2026) and among small businesses (from 5% in 2024/2025 to 12% in 2025/2026).

Incident response

Internal reporting remained the most common response following a breach or attack. Around eight in ten businesses (81%) and charities (84%) said they informed directors or trustees, and 62% of businesses and 73% of charities said they kept an internal record of the incident. External reporting was less common: among those identifying breaches or attacks, 40% of businesses and 36% of charities reported their most disruptive breach outside their organisation.

A smaller proportion of organisations already had formal incident response measures in place. In 2025/2026, the most common measures were roles or responsibilities assigned to individuals (39% of businesses; 31% of charities), written guidance on who to notify (34% businesses; 28% charities) and guidance on when to report externally (32% businesses; 30% charities). Formal incident response plans were less widespread (25% of businesses; 19% of charities), and these measures were more prevalent in larger organisations (for example, 57% of medium-sized businesses and 76% of large businesses had a formal incident response plan, compared with 21% of micro businesses).

Compared with 2024/2025, there were no meaningful year-on-year changes in the overall prevalence of these incident response measures for businesses or charities (for example, formal incident response plans were broadly stable at the overall level). The increases previously seen among small businesses were not repeated in 2025/2026, with small business levels broadly stable across key measures.

Following a breach or attack, 61% of businesses and 57% of charities reported taking some action to prevent future incidents, most commonly people or training changes (31% of businesses and 37% of charities).

Cyber Crime

Some cyber security breaches and attacks do not constitute cyber crimes under the Computer Misuse Act 1990 and the Home Office Counting Rules. Therefore, the statistics on prevalence and financial cost of cyber crime differ from the equivalent estimates for all cyber security breaches or attacks (as described above). They should be considered as a distinct set of figures, specifically for crimes committed against organisations, so are a subset of all breaches and attacks.

The survey estimated that 19% of businesses and 14% of charities have been victims of at least one cyber crime in the past year, accounting for approximately 267,000 businesses and 28,000 charities. Looked at another way, among the 43% of businesses and 28% of charities identifying any cyber security breaches or attacks, just under half (44% of businesses and 49% of charities) ended up being victims of cyber crime.

The larger the business, the more likely they were to experience cyber crime (17% of micro businesses, 24% of small businesses, 41% f medium businesses and 48% of large businesses). The same pattern was evident among charities with likelihood to experience cyber crime increasing with income (10% low-income charities, 18% medium-income charities, and 34% high-income charities).

The prevalence of cyber crime overall among businesses and charities remained relatively consistent with the previous two years (22% in 2023/2024, 20% in 2024/2025 and 19% in 2025/2026). However when looking at individual cyber crimes, among all charities there was a decrease in hacking cyber crime (from 2% in 2024/2025 to 1% this year) and an increase in ransomware cyber crimes (from less than 0.5% in 2024/2025 to 1% this year).

There may be signs of sector specific improvements, namely in the information and communication sector. Whilst prevalence of cyber breaches or attacks remained in line with last year (63% this year compared to 69%

last year), the proportion of businesses in the sector experiencing a cyber crime has decreased by almost half (from 43% in 2024/2025 to 22% this year), suggesting that defences against the most serious cyber breaches or attacks could be strengthening in the information and communication sector.

Phishing cyber crime remained the most prevalent type of cyber crime (accounting for 93% of businesses and 95% of charities that experienced a cyber crime), equating to 18% of all businesses and 13% of all charities, while other forms were less common.

Given phishing cyber crime dominates overall cyber crime, it was interesting to look at prevalence of non-phishing cyber crime. This year 3% of businesses and 2% of charities experienced a non-phishing related cyber crime, also in line with the previous two years among businesses (3% in 2023/2024 and 4% in 2024/2025) and among charities (2% in 2023/2024 and 3% in 2024/2025).

The median number of cyber crimes experienced in the last 12 months, was three cyber crimes for both businesses and charities. This remains roughly in line with last year where the median number experienced was four cyber crimes for both businesses and charities. Taking the mean estimates, businesses and charities both experienced 19 cyber crimes of any kind in the last 12 months. This data indicates a high level of repeat victimisation amongst some organisations experiencing cyber crime.

Using mean number of cyber crimes[footnote 2], it was estimated that UK businesses have experienced approximately 5.19 million cyber crimes of all types including approximately 70,000 non-phishing cyber crimes in the last 12 months. UK charities have experienced approximately 525,000 cyber crimes of all types in the last 12 months.

The median perceived cost of cyber crime other than phishing was £250, including those giving a cost of £0, and £750 excluding those giving a cost of £0. The range where most perceived costs fell (25th to 75th percentile) was £0 to £3,000 including £0 costs and £250 to £5,000, excluding £0 costs. The top 10% of perceived costs (90th percentile) ranged from £5,000 for those including £0 costs to £7,500 for those excluding £0 costs. While the report focuses on median costs and percentile ranges to reflect the experiences of most organisations, it is important to note that high-cost cyber crime incidents do occur. These incidents tend to be rare, highly variable in nature and often organisation-specific, which makes them persistently difficult to measure robustly within a survey of this size. As a result, extreme costs are not always fully reflected in the headline statistics, particularly where disclosure or reliability thresholds limit the reporting of upper percentiles.

An estimated 3% of all businesses and 1% of all charities have been a victim of fraud that resulted from a cyber breach or attack (cyber-facilitated fraud) in the last 12 months, equating to approximately 43,000 businesses

and 3,000 charities. There were an estimated 130,000 cyber-facilitated fraud events across the UK business population in the last 12 months.

Among businesses experiencing cyber-facilitated fraud, including costs of £0, the median perceived cost was £110, with the range of perceived cost where most fell (25th to 75th percentile) ranging from £0 to £2,000. Among those who had a cost associated with cyber-facilitated fraud, the median perceived cost was £500, with the range of perceived cost where most fell (25th to 75th percentile) ranging from £150 to £5,000. The perceived cost in the top 10% of cases was £12,000 including those with a £0 cost and £15,000 when excluding £0 costs. This paints a similar picture to cyber crime costs, that whilst the majority of businesses do not experience very high costs associated with cyber-facilitated fraud, a minority of businesses do face high costs.

Chapter 1: Introduction

1.1 Code of practice for statistics

The Cyber Security Breaches Survey is labelled as official statistics and has been produced to the standards set out in the Code of Practice for Statistics (https://code.statisticsauthority.gov.uk/).

In recent months the Office for Statistics Regulation (OSR) have carried out a compliance review (https://osr.statisticsauthority.gov.uk/publication/compliance-review-of-statistics-from-the-cyber-security-breaches-survey/) of these statistics which found that the statistics from the Cyber Security Breaches Survey were clear and insightful, and that the DSIT team has a good understanding of user needs. Given this review only concluded one month before this publication, the recommendations will mostly be considered for implementation next year. Users will continue to be engaged to identify any evidence gaps in this publication.

1.2 Background

Publication date: 30 April 2026

Geographic coverage: United Kingdom

The Department for Science, Innovation and Technology (DSIT), in partnership with the Home Office, commissioned the Cyber Security Breaches Survey of UK businesses, charities and education institutions. The findings of this survey provide a comprehensive description of cyber security for a representative sample of UK organisations, which provides a snapshot of UK cyber resilience at this point in time[footnote 3]. It tells us about the cyber threats organisations face and the actions they are taking to stay secure. It also supports the government to shape future policy in this area.

Since 2022/2023 the study has included estimates of cyber crime, and fraud that occurred as a result of cyber breaches or attacks (see Chapter 6). Some of the survey questions relating to these estimates were significantly changed for the 2023/2024 survey but remain broadly consistent this year. This means cyber crime results this year can be compared against 2024/2025 and 2023/2024 but not against 2022/2023 or before. Full details of all questionnaire changes between years are available in the Technical Annex. (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report)

These cyber crime statistics should ideally be considered alongside other related evidence on computer misuse, such as the general public statistics from the Crime Survey for England and Wales (https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest) (CSEW). The Cyber Security Breaches Survey adds to this evidence by looking at these types of crimes across businesses and charities.

The research was conducted by the independent research organisation, Ipsos. The project requirements and reporting are approved by Department for Science, Innovation and Technology and the Home Office. The 2025/2026 publication includes coverage of the following areas:

- prioritisation, information seeking (including use of government guidance) and decision making on cyber security, including among organisations' management boards
- cyber security approaches, covering risk management (including cyber insurance, software and supply chain risks), technical controls, the use of AI (including whether organisations had specific practices in place to manage the risks from the use of AI technology), whether personal data is protected, staff training and responsibilities and governance (including what is included in internal cyber security updates and internal cyber security audits)
- the cyber threat landscape, including identification of cyber security breaches or attacks, their outcomes and impacts, their self-reported financial cost

- incident response approaches and reporting of cyber security breaches or attacks
- the prevalence, nature, scale and financial costs of cyber crime, as well as the prevalence, nature and scale of fraud that occurred as a result of cyber breaches or attacks

This 2025/2026 publication follows previous surveys in this series, published annually since 2015/2016. In each publication year, the quantitative fieldwork has taken place towards the end of the preceding year.

This Statistical Release focuses on the business and charity outcomes. The results for educational institutions have been included in a separate Education Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings).

1.3 Methodology

As in previous years, there were two strands to the 2025/2026 Cyber Security Breaches Survey:

- Between August to December 2025, we undertook a random probability telephone and online survey of 2,112 UK businesses, 1,085 UK registered charities and 577 education institutions. 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 October and November 2025, to gain further qualitative insights from some of the organisations that answered the survey.

Sole traders and public-sector organisations (excluding education) are outside the scope of the survey. In addition, businesses with no IT capacity or online presence were deemed ineligible. These exclusions were consistent with previous years, and the survey is considered comparable across years where questions remain the same or very similar. Please see Sections 4.1 and 6.1 for notes on comparability of the prevalence of breaches or attacks and cyber crime across years.

The educational institutions, covered in the separate Education Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings), comprise 273 primary schools, 222 secondary schools, 33 further education colleges and 49 higher education institutions.

More technical details and a copy of the questionnaire are available in the separately published Technical Annex. (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report)

1.4 Changes since the 2024/2025 survey

The core approach for the 2025/2026 study - data collected from organisations via a random-probability survey, predominantly conducted by telephone, was unchanged from the previous years. However, one change was made to the weighting approach for businesses. In previous years of the survey, business data was weighted by size and sector. This year some regions (including the Devolved Nations and the North East of England) were oversampled to boost interviews in these regions, to allow for more robust analysis by region. Consequently, this year region weighting was also applied to businesses (as well as size and sector) to ensure that the regional profile of businesses matched the overall UK business population.

As such, we were still able to make comparisons to previous years where questions have remained the same or very similar.

Whilst there were no changes to the methodology between 2024/2025 and 2025/2026, there were some changes to the questionnaire. Key changes included:

- Adding questions to capture new areas of interest where insight was required (such as on the use of AI and the protection of personal data)
- Minor wording updates to existing questions to improve understanding and options available to respondents
- Minor routing changes to improve the flow of the interview
- Increasing the upper limit at numerical questions so higher values could be captured and adding in of some soft checks to accurately capture a range of responses

Full details of the questionnaire's changes and comparability with previous years are covered in the Technical Annex. (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report)

1.5 Naming convention for reference period of the Cyber Security Breaches Survey

For this year's survey, DSIT and the HO decided to update the naming convention used for reference periods for the Cyber Security Breaches Survey from a single year label (e.g. CSBS 2025) to a dual-year format (that is, CSBS 2025/2026 or CSBS 2025 to 2026). This change aims to reduce confusion, as previously the survey's title aligned with the year of publication but did not typically align with when the fieldwork was conducted, potentially misleading users about the timeframe of the findings. The dual-year approach reflects common UK government reporting practices, especially for activities spanning two calendar years or fiscal years.

Table 1.1 maps how previous CSBS surveys and fieldwork periods relate to the labelling convention in this year's report.

Table 1.1: CSBS survey references and fieldwork dates

Previous survey reference	Fieldwork period	Updated survey reference
CSBS 2016	November 2015 to February 2016	CSBS 2015/2016
CSBS 2017	October 2016 to January 2017	CSBS 2016/2017
CSBS 2018	October 2017 to December 2017	CSBS 2017/2018
CSBS 2019	October 2018 to December 2018	CSBS 2018/2019
CSBS 2020	October 2019 to December 2019	CSBS 2019/2020
CSBS 2021	October 2020 to January 2021	CSBS 2020/2021
CSBS 2022	October 2021 to January 2022	CSBS 2021/2022
CSBS 2023	September 2022 to January 2023	CSBS 2022/2023
CSBS 2024	September 2023 to January 2024	CSBS 2023/2024
CSBS 2025	August 2024 to December 2024	CSBS 2024/2025

Previous survey reference	Fieldwork period	Updated survey reference
CSBS 2025/2026	August 2025 to December 2025	CSBS 2025/2026

1.6 Interpretation of findings

How to interpret the quantitative data
The survey results are subject to margins of error, which vary with the size of the sample and the percentage figure concerned. For all percentage[footnote 4] results, differences are described[footnote 5] only where statistically significant (at the 95% level of confidence).[footnote 6] This includes comparison by size, sector, and previous years. By extension, where we do not comment on differences across years, for example where they are displayed in line charts, this was specifically because they may or may not be statistically significant differences. Where we use the term 'consistent' or 'in line' to describe trend data this indicates that there are no significant differences between the years being described.

Values greater than 0% but too small to be rounded up to 1% are shown as <0.5% or referred to as less than 0.5%.

While data presented throughout the survey is weighted, the base sizes presented on charts and tables are unweighted.

There is a further guide to statistical reliability at the end of this release.

How the extrapolations in this report have been calculated is included in Section 1.9 of the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report).

As noted throughout the report, the survey questionnaire included both 'prompted' and 'unprompted' questions. A prompted question is where the respondent is given a list of possible answers and is asked to choose from this list. An unprompted question asks the respondent to answer in their own words. In general, a prompted question is more appropriate where the possible answers are more clearly defined or known in advance, whereas an unprompted question is more exploratory and produces a wider range of answers.

Subgroup definitions and conventions
For businesses, analysis by size splits the population into:

- micro businesses (1 to 9 employees)
- small businesses (10 to 49 employees)
- medium businesses (50 to 249 employees)
- large businesses (250 or more employees)

For charities, analysis is considered in terms of annual income band, specifically looking at the subgroups of:

- low-income charities (annual income of less than £100,000)
- medium-income charities (annual income between £100,000 and £499,999)
- high-income charities (annual income of £500,000 or more)

Due to the relatively small sample sizes for certain business sectors, these have been grouped with similar sectors for more robust analysis. Business sector groupings referred to across this report, and their respective SIC 2007 sectors, are:

- administration or real estate (L and N)
- agriculture, forestry, or fishing (A)
- construction (F)
- education (P)[footnote 7]
- health or social care (Q)
- entertainment, service, or membership organisations (R and S)
- finance or insurance (K)
- food or hospitality (I)
- information and communication (J)
- utilities or production (including manufacturing) (B, C, D and E)
- professional, scientific or technical (M)
- retail or wholesale (including vehicle sales or repairs) (G)
- transport or storage (H)

Analysis of organisation cyber security split by geographical region was considered to be out of the scope of this reporting. While we may occasionally provide data specific for UK regions (at International Territorial Level 1), we recommend caution in attributing these differences to actions taken or not taken by that region given regional differences may also be attributable to the size and sector profile of the sample in that region.

Where figures in charts do not add to 100%, or to an associated net score, this is due to rounding of percentages or because the questions allow more

than one response.

From the 2022/2023 survey onwards, for businesses and charities, we substantially increased the use of split-sampling, where certain questions were only asked to a random half of the sample, in order to maintain questionnaire length whilst adding in new questions ('half A' randomly gets assigned half of the split-sampled questions and 'half B' randomly gets assigned the other split sampled questions). For the same reason we also restricted various questions to larger organisations (medium and large businesses, and high-income charities). Where charts are based on split-sampled questions the base label will specify whether those answering were 'half A' or 'half B' to denote that the question was only asked of half the sample.

How to interpret the qualitative data
The qualitative findings offer more nuanced insights into the attitudes and behaviours of businesses and charities with regards to cyber security. The findings reported here represent common themes emerging across multiple interviews. Insights and verbatim quotes from individual organisations are used to illustrate findings that emerged more broadly across interviews. However, as with any qualitative findings, these examples are not intended to be statistically representative.

1.7 Acknowledgements

Ipsos, DSIT and the Home Office would like to thank all the organisations and individuals who participated in the survey. We would also like to thank the organisations who supported the survey development work, endorsed the fieldwork, and encouraged organisations to participate, including:

- the Association of British Insurers (ABI)
- TechUK
- Jisc, a not-for-profit company that provides digital infrastructure, services, and guidance for UK further and higher education institutions
- UCISA (formerly known as the Universities and Colleges Information Systems Association)
- National Cyber Security Centre (NCSC)

Chapter 2: Awareness and attitudes

This chapter explores:

- prioritisation of cyber security within organisations
- receiving and reacting to information and guidance about cyber security
- qualitative data on how organisations make decisions on cyber security

Key takeaways

- Cyber security remained a high priority for senior management in around seven in ten businesses (72%) and six in ten charities (60%). Whilst this was broadly consistent with last year for businesses, for charities, the proportion treating cyber security as a high priority has declined significantly from 2024/2025, down from 68% to 60%. Low-income charities (with an income of £0 to less than £100,000), drove the decline, with their prioritisation decreasing from 64% in 2024/2025, to 53% in 2025/2026.
- Board-level responsibility for cyber security sat at 31% of businesses and 30% of charities and continued to be higher in larger businesses (68% of large businesses). Compared to last year, the proportion among businesses has increased (from 27%), reversing the longer-term downward pattern seen earlier in the decade.
- Seeking external information or guidance was reported by 44% of businesses and 31% of charities. This was most common among medium businesses (71%) and small businesses (58%), compared with 41% of micro businesses. For charities, this also reflects a decline compared with 2024/2025, aligning with the wider picture of reduced prioritisation in this wave mentioned above.
- The most common individual source of advice was external cyber security/IT consultants or providers (27% of businesses and 13% of charities). This was higher among medium (51%) and small businesses (39%) than micro businesses (24%).
- Awareness of government initiatives increased compared with last year, reversing the longer-term decline seen previously: Cyber Aware was recognised by 30% of businesses and 30% of charities, while awareness of 10 Steps was 17% (businesses) and 19% (charities), and Cyber Essentials was 17% (businesses) and 16% (charities).
- The Cyber Governance Code of Practice (launched in April 2025), had been heard of by 16% of charities and businesses. Launched in May 2025, the Software Security Code of Practice was recognised by 22% of businesses and 19% of charities.

2.1 Perceived importance of cyber security

Around seven in ten businesses (72%) reported that cyber security was a high priority for their senior management. A lower proportion of charities, (60%) said the same (Figure 2.1).

In interpreting this question, note that in smaller organisations, the individuals responsible for cyber security, i.e. those who completed this survey, tend to be senior management themselves, so are answering with regards to their own views. In larger organisations, these individuals may not be part of senior management, so their answers will reflect their own perceptions of their senior management team's views.

Figure 2.1 : Extent to which cyber security was seen as a priority for directors, trustees, and other senior managers

Change to table view

Organisation type	% Very High	% Fairly High	% Fairly Low	% Very Low	% Don't Know	Total
Businesses	34	38	20	7	1	
Charities	21	39	24	15	1	

Bases: Split-sample half A: 1,051 businesses, 530 charities
Note: Percentage labels are not always shown for some small categories due to space

It was more common for larger businesses to say that cyber security was a high priority (100% of large businesses and 92% of medium businesses compared with 72% of businesses overall). In contrast almost a third of micro businesses (30%) deemed cyber security a low priority (compared to 8% of medium businesses and 0% of large businesses). The same was true for charities, where high-income charities were more likely to see cyber security as a high priority (87% of charities with an income of £500,000 or more compared with 60% of charities overall). This continued the pattern observed since 2019/2020, where larger organisations tended to treat cyber security more seriously.

Businesses in the following sectors treated cyber security as a higher priority than businesses overall:

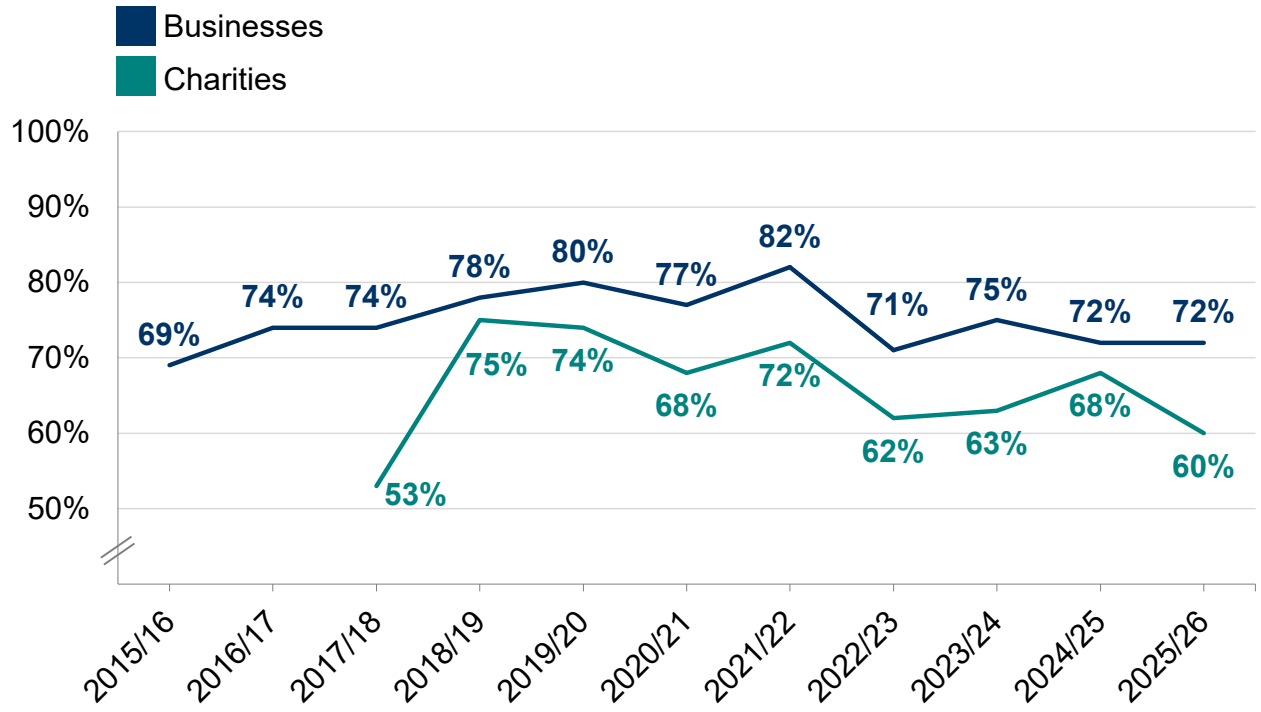
- finance or insurance (89% said it was a high priority)
- professional, scientific or technical (85% said it was a high priority)
- administration or real estate (83% said it was a high priority)

Trends over time

Figure 2.2 shows how the prioritisation of cyber security in organisations has changed over time. For businesses, the prioritisation of cyber security in 2025/2026 has remained in line with the previous two years (2024/2025 and 2023/2024).

For charities, the proportion treating cyber security as a high priority has declined significantly from 2024/2025, down from 68% to 60%. This was a reversal of a slight upward trend seen between 2023/2024 and 2024/2025, taking this measure to its lowest for charities since 2017/18. Smaller charities (with an income of £0 to less than £100,000), drove the decline, their prioritisation decreasing from 64% in 2024/2025, to 53% in 2025/2026. In contrast, the measure was steady for charities with larger incomes. It was 81% in 2025/2026 for medium-income charities (consistent with 75% in 2024/2025), and 87% in 2025/2026 for high-income charities (consistent with 88% in 2024/2025).

Figure 2.2: Percentage of organisations over time where cyber security was seen as a high priority for directors, trustees, and other senior managers



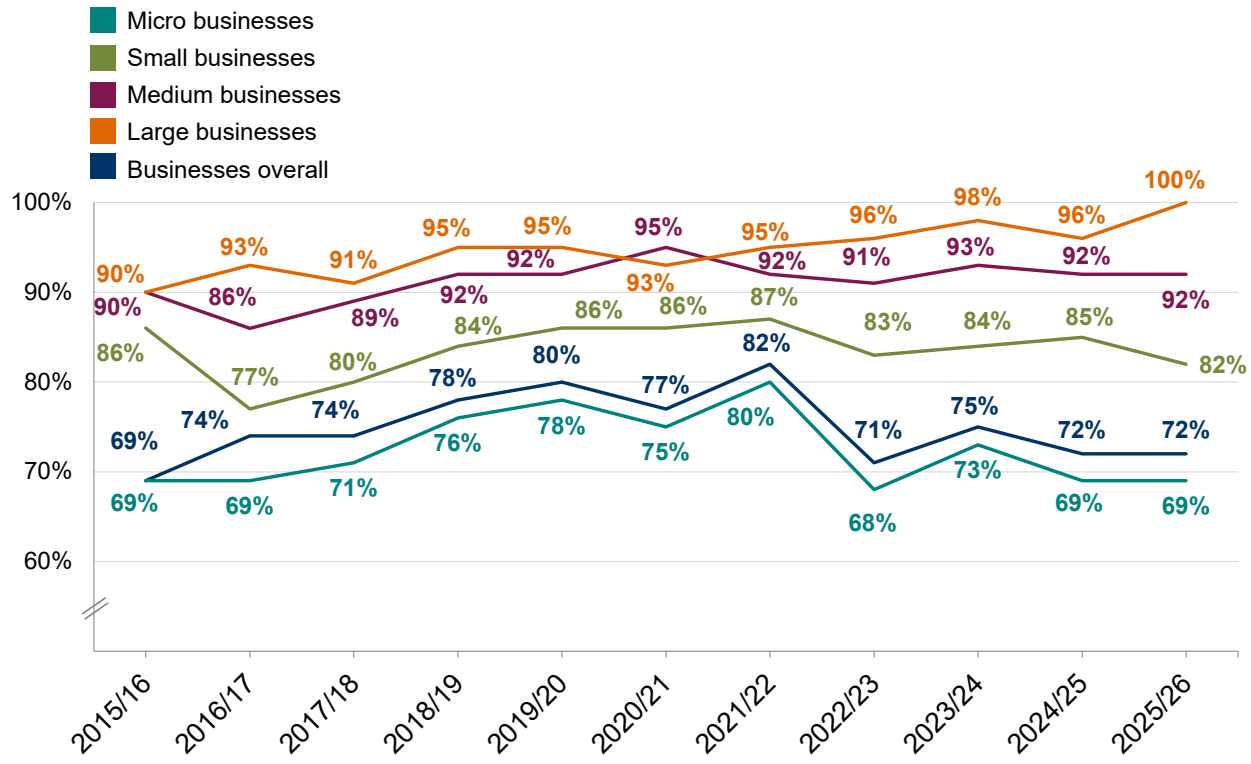
Bases: c.1,000+ businesses per year; 450+ charities per year (split sample half A from 2023 onwards).

Figures 2.3 and 2.4 show the percentage of businesses and charities where cyber security was seen as a high priority, by business and charity size

(charities were first surveyed in 2018 and therefore have no data points before this time).

For businesses, there has been no significant changes, compared with 2024/2025 (Figure 2.3).

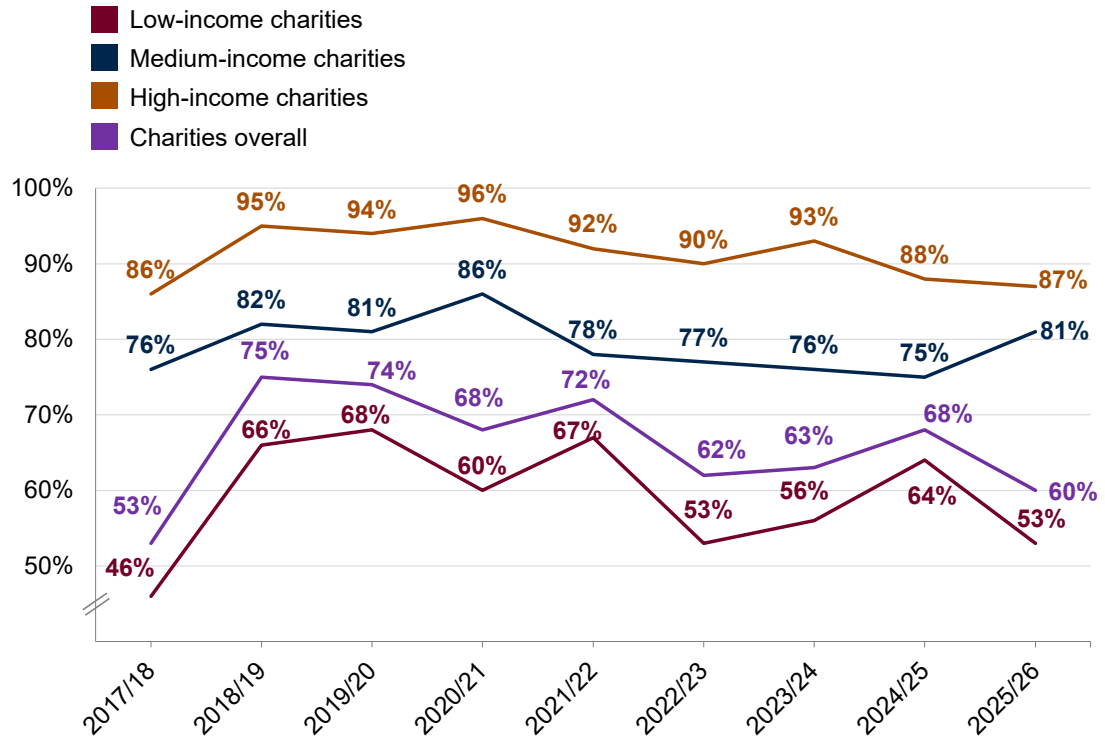
Figure 2.3: Percentage of businesses, by size, over time where cyber security was seen as a high priority for directors, trustees, and other senior managers



bases per year: c.1,000+ businesses overall; c. 550+ micro businesses; c. 240+ small businesses; c. 120+ medium businesses; c. 85+ large businesses (split sample half A from 2022/2023 onwards)

For charities, the picture was mixed (Figure 2.4). Whilst medium (81%) and high-income (87%) charities continued to overwhelmingly describe cyber security as a high priority, there has been a significant decrease in the proportion of low-income charities describing it as high priority (53%) compared to 2024/2025 (64%). This has contributed to a decrease in charities overall describing cyber security as a high priority (from 68% in 2024/2025 to 60% this year).

Figure 2.4: Percentage of charities, by size, over time where cyber security was seen as a high priority for directors, trustees, and other senior managers



bases per year: c.450+ charities overall; c. 100 low-income charities; c. 50 medium-income charities; c. 80 high-income charities (split sample half A from 2022/2023 onwards)

Qualitative insights on cyber security prioritisation

When prompted to identify the top two or three cyber priorities in the past 12 months, qualitative respondents frequently mentioned:

- The prevalence of phishing and impersonations
- The goal of moving towards Cyber Essentials or Cyber Essentials Plus accreditations
- The challenges associated with cyber security awareness and training within organisations
- The impact of artificial intelligence on cyber security (see section 3.1 for more detail on AI and cyber security)
- The prioritisation of a digital transformation or update, especially if systems were older

In addition, awareness of cyber risks and the economic conditions were explored.

Firstly, there was a common perception that reports of large-scale attacks influenced cyber security discussions within organisations. These reported attacks were raised spontaneously by all organisation types and sizes.

> "I would say our awareness of cyber resilience and risks is quite heightened at the minute because it's been in the news a lot, the big

> attacks in the retail sector. HR recently attended a cyber function with several sectors, and it was quite a hot topic." **Large business, Real estate**

Secondly, some organisations thought that the economic climate put additional pressure on cyber budgets. This seemed particularly prominent among smaller organisations.

> "Everything that's going on economically in the country has put a lot of strain on the company in general. Which means we can't just say okay well here's 18 grand, go and buy new computer systems." **Small business, Health and social care**

2.2 Involvement of senior management

How often are senior managers updated on cyber security?
Figure 2.5 breaks down how often senior managers were given updates on actions around cyber security. The question was restricted to medium and large businesses, and to high-income charities since 2022/2023.

Larger businesses were consistent with last year's results, with 83% receiving updates at least annually, and 81% at least quarterly (consistent with 91% and 83% in 2024/2025, respectively). However, amongst medium businesses, there was a significant decline from 2024/2025 to 2025/2026 in senior management being given updates on cyber security at least annually (78%, declining to 70%).

Charities, similar to medium businesses, also saw a significant decline in the proportion receiving updates at least annually, from 78% in 2024/2025 to 69% in 2025/2026.

Figure 2.5 : How often directors, trustees or other senior managers are given an update on any actions taken around cyber security

Change to table view

Frequency of updates	% At least monthly	% Quarterly	% Annually	% Less than once a year	% Each time there is a breach or attack	% Never	
Medium businesses	41	16	13	3	16	5	
Large businesses	52	29	2	1	12	0	
High-income charities	21	29	19	3	16	6	

Bases: 296 medium businesses; 155 large businesses; 335 high-income charities
Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

The content of updates

A new question was added to CSBS in 2025/2026 covering the content of any cyber security updates shared with directors, trustees or other senior managers. It was asked of medium and large businesses and high-income charities, who had said they provided any cyber security updates. They were prompted on whether their updates included:

- Management of cyber security risk; included in updates by 79% of businesses and 84% of charities
- Investments in cyber security; 69% of businesses, and a significantly lower 60% of charities
- Approach to developing cyber skills within the organisation; 64% of businesses and 65% of charities
- Types of attacks detected; 66% of businesses and 68% of charities
- Number of significant attacks detected; 61% of businesses and 62% of charities

Board responsibilities

Around three in ten businesses (31%), and a similar proportion of charities (30%), had board members or trustees taking explicit responsibility for cyber security as part of their job (Figure 2.6). This was asked across all organisations. Note that while all registered charities have boards of

trustees, not all businesses have a formal management board, which may artificially reduce business response on this measure.

As might be expected, board-level responsibility was much more common in larger businesses, where the management board was likely to be larger. More than two-thirds of large businesses (68%) had a board member responsible for cyber security compared with 31% of businesses overall.

Figure 2.6 : Percentage of organisations with board members or trustees that have responsibility for cyber security

Change to table view

Micro businesses	29%
Small businesses	37%
Medium businesses	52%
Large businesses	68%
Businesses overall	31%
Charities overall	30%

Bases: 1,154 micro businesses, 507 small businesses, 296 medium businesses, 155 large businesses; 2,112 businesses overall; 1,085 charities overall.

As shown in Figure 2.7, businesses in the finance or insurance (54%), information and communication (51%) and professional, scientific or technical (41%) sectors were each more likely than businesses overall to have board members taking responsibility for cyber security. The finance or insurance and professional, scientific or technical sectors were also among those most likely to prioritise cyber security (Section 2.1), and this was a trend that has been seen in previous years of the survey. At the other end of the scale, businesses in transport or storage (17%), retail or wholesale (20%) and construction (24%) sectors, were among the least likely to have board members assigned to this role. The retail or wholesale sector was also less likely to see cyber security as a priority.

Figure 2.7 : Percentage of organisations with board members or trustees that have responsibility for cyber security, by sector

Change to table view

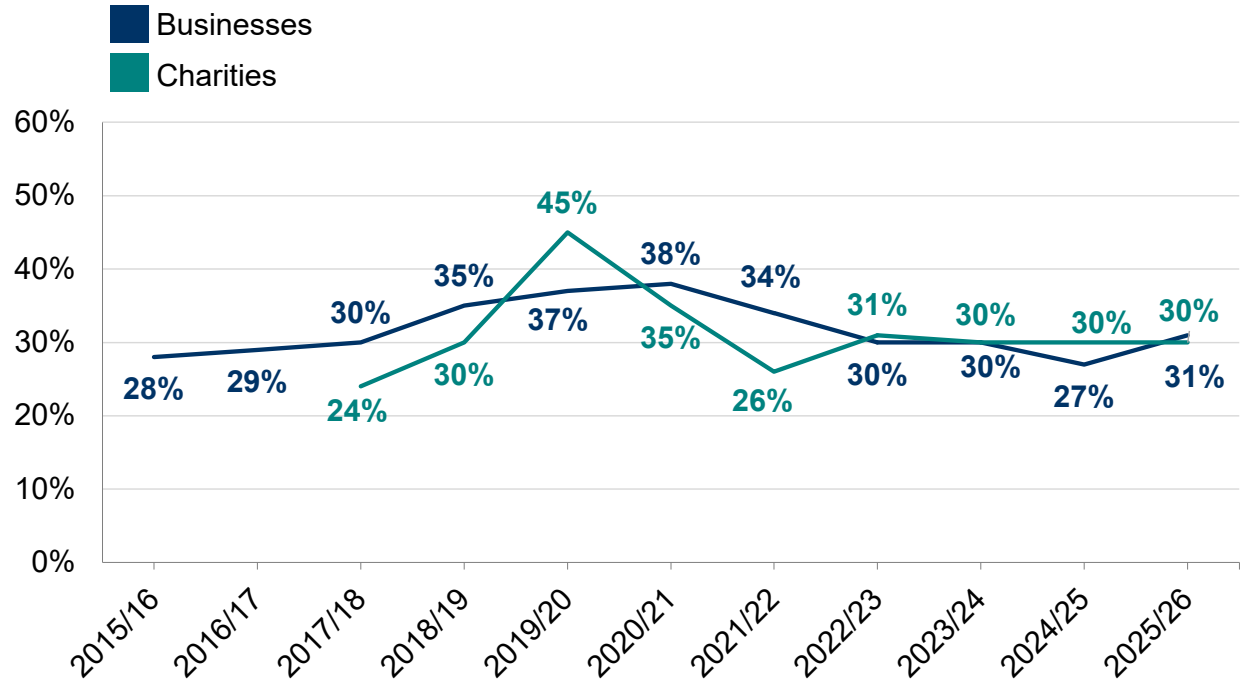
Finance or insurance	54%
Information and communication	51%
Professional, scientific or technical	41%
Health or social care	38%
Administration or real estate	36%
Utilities or production	33%
Food or hospitality	30%
Entertainment or service	24%
Construction	24%
Agriculture, forestry or fishing	24%
Retail or wholesale	20%
Transport or storage	17%
Businesses overall	31%

Bases: 101 finance or insurance businesses; 81 information and communication businesses; 217 professional, scientific or technical businesses; 205 utilities or production businesses; 101 health, social care or social work businesses; 306 administration or real estate businesses; 85 transport or storage businesses; 302 retail or wholesale (including vehicle sales and repairs) businesses; 163 entertainment, service or membership organisations; 262 construction businesses; 184 food or hospitality businesses; 2,112 businesses overall.

Trends over time

Figure 2.8 shows the trend over time for board members having specific cyber security responsibilities. This year, the proportion of businesses with board member responsibility has increased, from 27% to 31%, reversing a trend of decline between 2020/2021 and 2024/2025. For charities, results have remained stable, at 30%, for the past three years.

Figure 2.8: Percentage of organisations over time with board members or trustees with responsibility for cyber security



Bases: c.1,000+ businesses per year; 500+ charities per year

Qualitative insights on formal versus informal board engagement
There was a sense that board members were generally more aware and engaged in the cyber security posture of their organisation than they might have been previously. The increase in engagement tended to be linked to a number of high-profile cyber security breaches and attacks and cyber crimes reported in the media.

> "The board is a lot more aware and focused on cyber security risks than they were prior. Not from a single event, but the building cadence of catastrophic stories. The board's risk appetite has probably descended, i.e. they don't want to take as much risk as they had done in in the past." **Large business, Information/communication**

> "Our CEO started asking a lot of questions following the [publicised cyber-crime] case." **Medium business, Wholesale/retail**

Challenges, however, remained and personal characteristics of board members were often seen as contributing to their cyber involvement. For example, some IT managers felt they were trusted by senior leaders because the owner was older and therefore did not have high awareness of organisational cyber needs. One small business said that their close personal relationship with the senior leadership team allowed for productive conversations about cyber. Another smaller business mentioned that senior leadership changed and trying to engage with a new contact was a challenge.

> “Will he [older boss] understand what I'm telling him? Probably not.” **Medium business, Transport or storage**

Whilst board engagement was typically on the rise over the past 12 months, some organisations were more sceptical about whether high profile incidents led to any changes or just general awareness. Systematic discussions with senior leadership appeared to be mixed. Large-scale news stories sometimes did not lead to full ownership taken by senior leadership about potential cyber breach impacts.

> “I don’t know that they think about cyber security, they just want to tell clients we are secure.” **Small business, Professional/scientific/technical**

2.3 Sources of information

Overall proportion seeking cyber security information or guidance
External sources of information and guidance on cyber security included government sources, third-party cyber security or IT providers, and trade bodies, as well as information found through an internet search or from the media. More than four in ten businesses (44%), and almost three in ten charities (31%), reported actively seeking external information or guidance on cyber security from outside their organisation in the past year (Figure 2.9).

Small (58%) and medium (71%) businesses were most likely to seek out external information, as were medium-income charities with an income of between £100,000 and £500,000 (56%) and high-income charities with an income of £500,000 or more (72%).

Figure 2.9 : Proportion of organisations that have sought external information or guidance in the last 12 months on the cyber security threats faced by their organisation

Change to table view

Micro businesses	41%
Small businesses	58%

Medium businesses	71%
Large businesses	61%
Businesses overall	44%
Charities overall	31%

Bases: Split-sample half A: 580 micro businesses; 241 small businesses; 154 medium businesses; 76 large businesses; 1,051 businesses overall; 530 charities overall.

Business results were in line with 2024/2025 and prior years (42% sought external advice in 2024/2025, against 44% in 2025/2026). However, this remained lower than the highpoints recorded for businesses in 2022/2023 (49%) and 2021/2022 (48%). For low-income charities, there was a significant decline in the proportion seeking any external guidance, from 32% in 2024/2025, to 21% in 2025/2026. The aggregate figure for all charities was 37% in 2024/2025 and 31% 2025/2026, but this was not a statistically significant decrease.

Figure 2.10 highlights the proportion of businesses in each sector seeking external information and guidance. Businesses in the finance or insurance (59%), administration or real estate (56%) and professional, scientific or technical sectors (54%), were more likely to have sought external information or guidance.

Figure 2.10 : Proportion of organisations that have sought external information or guidance in the last 12 months on the cyber security threats faced by their organisation, by sector

Change to table view

Finance or insurance	61%
Administration or real estate	56%
Professional, scientific or technical	56%
Utilities or production	43%
Entertainment or service	40%
Agriculture, forestry or fishing	37%

Retail or wholesale	37%
Food or hospitality	36%
Construction	35%
Transport or storage	26%
Businesses overall	44%

Bases: Split-sample half A: 50 finance or insurance businesses; 154 administration or real estate businesses; 56 health, social care or social work businesses; 116 professional, scientific or technical businesses; 93 utilities or production businesses; 88 entertainment, service or membership organisations; 36 agriculture, forestry or fishing businesses; 139 retail or wholesale (including vehicle sales and repairs) businesses; 92 food or hospitality businesses; 124 construction businesses; 1,051 businesses overall.

Where do organisations get information and guidance?
As in previous years, the most common individual sources of information and guidance were:

- external cyber security consultants, IT consultants or cyber security providers (mentioned by 27% of businesses and 13% of charities)
- internal sources within the organisation such as colleagues, in-house experts and the management board (6% of businesses and 6% charities)
- any government or public sector source, including government websites, regulators, and other public bodies (4% of businesses and 4% charities)
- general online searching (4% of businesses and 3% of charities)

To note, this question was unprompted for those doing the survey by telephone (the vast majority, 94% of all organisations), while those doing it online looked at a prompted response list.

Consistent with previous years, few organisations named specific official bodies. For example, 1% of businesses and 1% of charities mentioned the National Cyber Security Centre (NCSC) by name. Among charities, 3% mentioned the Charity Commission (England and Wales, Scotland or Northern Ireland). This continues to indicate that organisations are more likely to rely on external providers than to cite official or sector-specific bodies by name.

There were some notable statistically significant differences by business size:

- Use of external consultants/providers rose sharply with size: 24% of micro, 39% of small and 51% of medium businesses. Small and medium businesses were significantly more likely than micro businesses to use external providers, and medium businesses were significantly more likely than small businesses to do so
- Medium businesses were significantly more likely than small businesses to mention government/public sector sources (6% vs 2%)
- Among micro businesses, after external consultants/providers (24%), the next most common responses included online searching (4%) and their bank/bank IT staff (2%)

Awareness of government guidance, initiatives, and communications
The unprompted question on sources of information in the previous subsection was likely to under-state awareness of government cyber communications, because people often do not recall specific campaigns or products without prompting (especially in the telephone survey). We therefore asked organisations, in a later prompted question, whether they had heard of specific government initiatives or communications before. These included:

- the national Cyber Aware communications campaign, which offers tips and advice to protect individuals and small businesses against cyber crime
- the 10 Steps to Cyber Security guidance, which summarises how organisations can protect themselves by managing cyber risk
- the government-endorsed Cyber Essentials scheme, which enables organisations to be certified independently for having implemented technical good-practice in cyber security
- new for 2025/2026: the Cyber Governance Code of Practice, a framework designed to support boards of medium-to-large organisations effectively take ownership of managing cyber security risks
- new for 2025/2026: the Software Security Code of Practice, a voluntary code for technology providers which outlines security principles expected of any organisation that develops or sells software.

Cyber Aware was the most recognised of the initiatives listed above, with 30% of businesses and 30% of charities aware (Figure 2.11 and 2.12). Around one in five businesses were aware of the 10 Steps (17%) and Cyber Essentials (17%). Among charities, 19% were aware of the 10 Steps and 16% were aware of Cyber Essentials.

Of the two schemes newly covered in the 2025/2026 CSBS survey, the Cyber Governance Code of Practice was recognised by 16% of businesses and charities, and the Software Security Code of Practice by 22% of businesses and 19% of charities.

Awareness continued to be higher among larger businesses (note that estimates for large businesses should be treated with caution due to lower statistical reliability in this subgroup). In particular, both medium-sized and large businesses were significantly more likely than micro and small businesses to have heard of each initiative:

- Cyber Aware: 60% of large businesses, 44% of medium businesses, 30% of small businesses and 29% of micro businesses had heard of it (medium significantly higher than micro/small; large also significantly higher than micro/small/medium)
- 10 Steps: 49% of large businesses, 34% of medium businesses, 23% of small businesses and 15% of micro businesses were aware (small and medium significantly higher than micro)
- Cyber Essentials: 64% of large businesses, 56% of medium businesses, 25% of small businesses and 14% of micro businesses were aware (small and medium significantly higher than micro; medium also significantly higher than small)
- Cyber Governance Code of Practice: of businesses, 51% large, 32% medium, 18% of small and 14% micro had heard of this scheme (large businesses significantly higher than all other groups, medium businesses significantly higher than small and micro)
- Software Security Code of Practice: of businesses, 51% large, 29% medium, 23% small and 21% micro had heard of it (large businesses significantly higher than all other groups)

Looking at charities, a similar pattern was observed by income, with levels of awareness across all initiatives being significantly higher among high-income charities:

- 40% of charities with income £500,000+ had heard of Cyber Aware, compared to 30% of charities overall
- 34% of £500,000+ charities were aware of the 10 Steps guidance, compared to 19% overall
- 40% of £500,000+ charities were aware of Cyber Essentials, compared to 16% overall
- 29% of £500,000+ charities were aware of the Cyber Governance Code of Practice, compared with 16% overall
- 29% of £500,000+ charities were aware of the Software Security Code of Practice, compared with 19% overall

Qualitative insights on the use of cyber guidance

External influencers often played a key role in determining whether and how cyber guidance was used. Smaller businesses in particular indicated reliance on IT partners for guidance, and in some cases friends and family (often younger more ‘IT savvy’ family members) were called upon for

advice. This highlighted that businesses were either unaware of available guidance or lacked confidence in their ability to access or understand it.

> “But ultimately [the IT provider] has the final say in control, so that's where we go for help.” **CEO, Small business**

> “I spoke to the family, all the grandkids are sort of into it, so may have spoken to them and got recommendations, but again, they're way beyond me and go too deep.” **Proprietor, Micro business**

Larger businesses tended to have both external and internal governance and guidance for cyber security. Research publications, training and collaboration between employees and external consultants were cited as important forms of cyber guidance and governance.

Charities typically highlighted external resources that were free or low-cost, such as pro bono consultants.

> “We do have a number of pro bono consultants who have cyber security background and they provide knowledge and guidance where appropriate.” **Head of IT and systems, Charity**

Businesses and charities highlighted a desire for clear, tailored, and actionable cyber guidance from the government. Smaller businesses sometimes felt that guidance was tailored to larger systems and businesses which they did not understand and could not easily translate to their business. Simple step by step guides were seen as particularly important for smaller businesses to address this issue.

> “[Information] especially for a small business? It would be a really simple, ‘this is what you need to think about’ [cyber security] guide.” **Business owner, Small business**

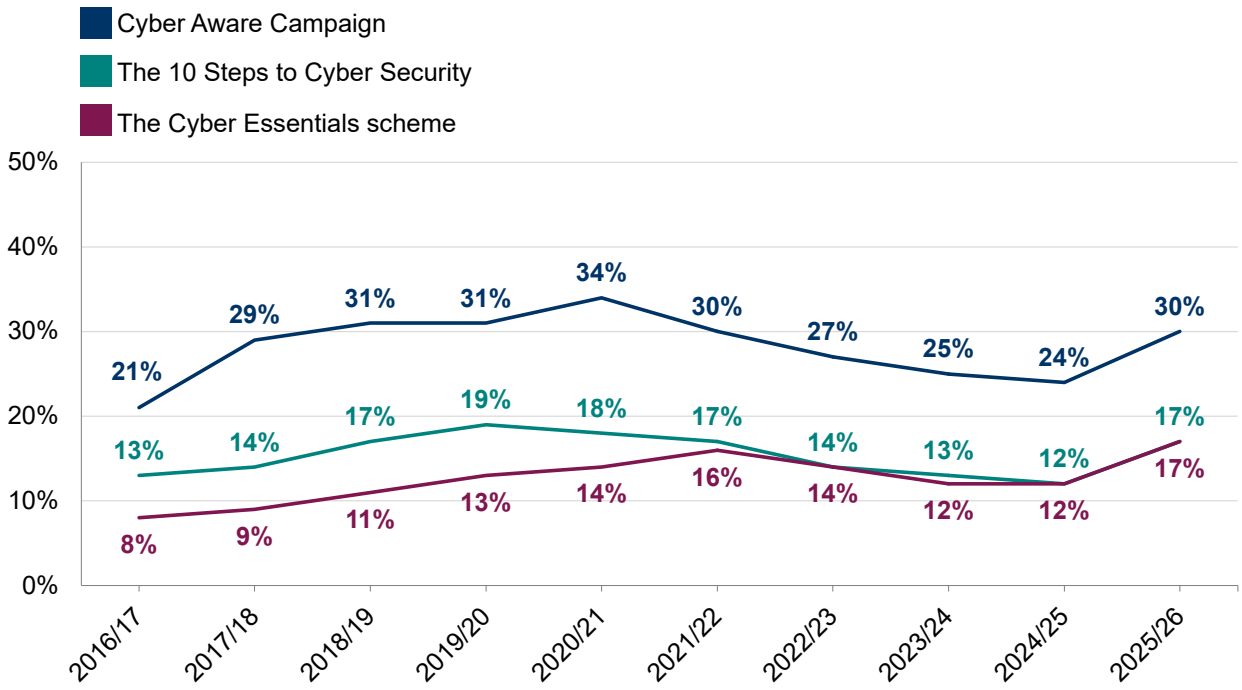
Some participants suggested that the NCSC should continue its current efforts but also exercised caution to avoid government advice saturation. Similarly, businesses did not always trust that government systems were completely secure, which raised some concerns around not always being able to trust that government guidance was really coming from the government. This saturation or mistrust of government information could lead to businesses and charities tuning out important messages.

> “You need to become more aware of [cyber guidance]. Is there a saturation point with government? I think that's half the problem… they need to make sure their own systems are safe.” **Quality and IT Manager, Medium business**”

Trends over time

Figure 2.11 illustrates that business awareness of each of these initiatives has changed little over the last 10 years. Prior to 2025/2026, there had been a steady decline in awareness of initiatives since 2020/2021. This year, there was a statistically significant increase in awareness on all three schemes displayed, compared with last year.

Figure 2.11: Percentage of businesses over time aware of the following government guidance, initiatives, or communication campaigns

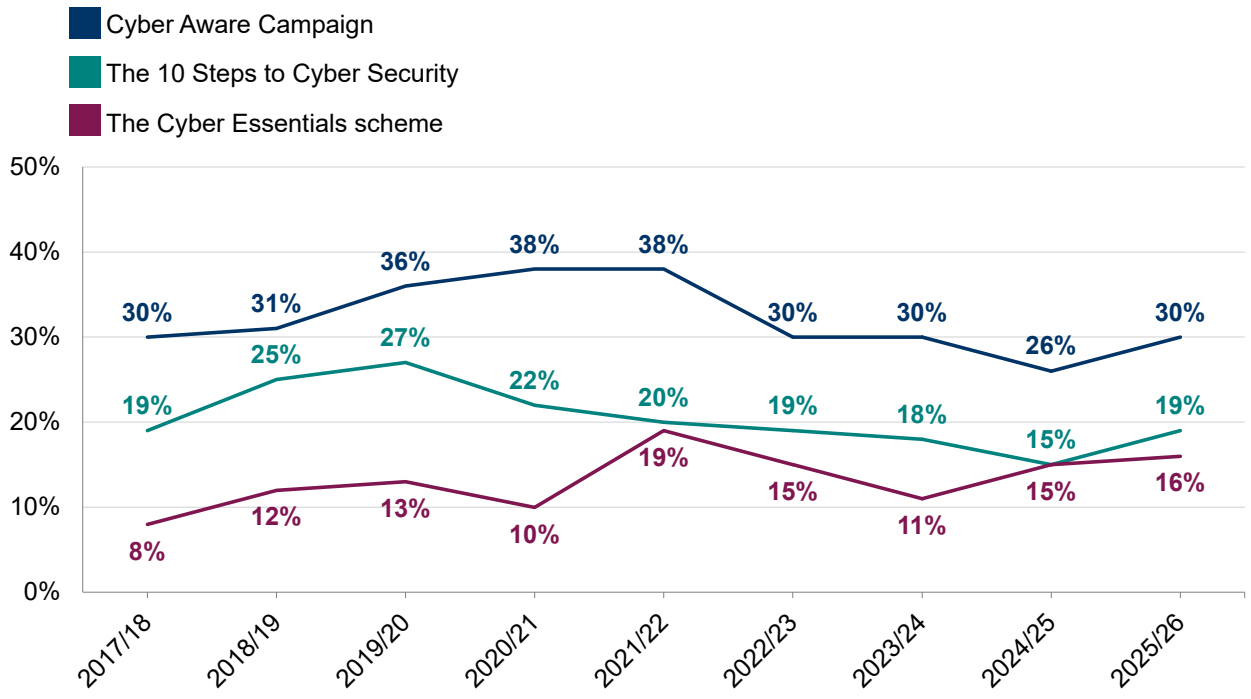


Bases: c.1,000+ businesses per year (split-sample half B from 2022/2023 onwards)

The increase in awareness of the Cyber Aware Campaign was driven by micro businesses, rising from 22% in 2024/2025 to 29% in 2025/2026.

For charities, there were signs that awareness may be on the increase. For example, 26% knew of Cyber Aware in 2024/2025, rising to 30% in 2025/2026 (see Figure 2.12 for full details), however none of these increases are statistically significant.

Figure 2.12: Percentage of charities over time aware of the following government guidance, initiatives, or communication campaigns



Bases: c.450+ charities per year (split-sample half B from 2022/2023 onwards)

Guidance targeted at specific types of organisations
Since 2020, the survey has asked about NCSC (National Cyber Security Centre) guidance that directed to specific sizes of business or towards charities. This included:

- the NCSC's Small Business Guide and Small Charity Guide, which outline more basic steps that these smaller organisations can take to protect themselves
- the NCSC's Cyber Security Toolkit for Boards (renamed for 2025/2026 from "the Board Toolkit"), which helps management boards to understand their obligations, and to discuss cyber security with the technical experts in their organisation

In 2025/2026, awareness of Small Business Guides among micro and small businesses remained relatively low, at 13% overall, including 13% of micro businesses and 17% of small businesses. This was in line with the previous wave (13% overall in 2025, including 11% of micro and 14% of small businesses).

Among charities this year awareness of the Small Charity Guide was 17%. Awareness was higher among high-income charities (£500,000+), at 29%, compared with charities overall. Levels were similar to 2024/2025 (15% among charities overall and 33% among high-income charities).

The Cyber Security Toolkit for Boards continued to be explored by medium and large businesses, as well as high-income charities. In 2025/2026, 20% of medium businesses, 36% of large businesses, and 19% of high-income charities were aware of the Toolkit.

In 2025/2026, awareness of the Cyber Security Toolkit for Boards was 23% among businesses overall, with large businesses more likely than average to have heard of it, on 36%. Among high-income charities, awareness was 19%. These were broadly in line with 2024/2025 (22% among businesses overall, 22% of medium businesses, 27% of large businesses and 17% of high-income charities).

Impact of government information and guidance
Overall, 58% of businesses and 59% of charities recalled seeing at least one of the government communications or guidance covered in the previous section when prompted, up from 38% of businesses and 46% of charities in 2024/2025.

Those aware of at least one form of government guidance were then asked about any changes they had made to their cyber security measures, in response to what they had seen. This year, 38% of these businesses and 35% of these charities reported making at least one change after seeing government guidance on cyber security.

One notable shift from last year was an increase in organisations saying they had done nothing after seeing or hearing government guidance. In 2025/2026, 46% of businesses and 51% of charities who had heard government guidance reported that nothing was done, compared with 39% of businesses and 35% of charities in 2024/2025.

Looking across business sizes (where bases are sufficiently robust), 49% of medium businesses reported making at least one change, compared with 36% of micro businesses.

In terms of the specific changes made, a wide variety of unprompted responses were given. In 2025/2026, the most commonly reported types of change among those who had heard government guidance included:

- Technical changes (23% of businesses and 20% of charities)
- People/training-related changes (17% of businesses and 11% of charities)
- Governance changes (11% of businesses and 15% of charities)

The top unprompted individual response categories in 2025/2026 were:

- Staff training and communications (7% of businesses and 8% of charities)
- Changing or updating firewalls or system configurations (7% of businesses and 6% of charities)
- New or updated antivirus/anti-malware software (6% of businesses and 5% of charities)
- Outsourced cyber security / hired an external provider (10% of businesses and 3% of charities)

Chapter 3: Approaches to cyber security

This chapter looks at the various ways in which organisations are dealing with cyber security and covers topics such as:

- risk management
- reporting cyber risks
- cyber insurance
- technical controls
- training and awareness raising
- staffing and outsourcing
- governance approaches and policies
- AI adoption and risk management
- supplier risk management

We also explore the extent to which organisations are meeting the requirements set out in the government-endorsed Cyber Essentials (https://www.ncsc.gov.uk/cyberessentials/overview) scheme and the government's 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security) guidance.

Key takeaways

- Last year in 2024/2025, small businesses were observed to have increased their actions on a number of cyber hygiene measures. However, in 2025/2026, this trend has reversed, with many measures returning to 2023/2024 levels:
  - a decrease in those undertaking cyber security risk assessments (41% down from 48% in 2024/2025)
  - a decrease in having a formal policy covering cyber security risks (52% down from 59% in 2024/2025)
  - a decrease in having a business continuity plan that covered cyber security (44% down from 53% in 2024/2025)
- Micro businesses, however, were observed to have seen some increases in their cyber security measures compared to 2024/2025:

    - an increase in those that only allow access via company-owned devices (64% up from 58% in 2024/2025)
    - an increase in those that require two-factor authentication (43% up from 35% in 2024/2025)
    - an increase in those with an external cyber security provider (44% up from 39% in 2024/2025) - whilst not necessarily an indicator of cyber hygiene, for micro businesses who typically do not have in house IT departments, it shows that cyber security was being invested in

- Whilst charities overall have remained consistent with last year on the majority of measures relating to approaches to cyber security, high-income charities have increased on some measures compared to 2024/2025. This includes the proportion that considered cyber security to a large extent when purchasing software (45% up from 37% in 2024/2025) and the proportion that had some form of cyber insurance (75% up from 64% in 2024/2025).
- Around seven in ten large businesses (74%) and just under six in ten medium businesses (57%) have a cyber security strategy in place, consistent with 2024/2025 (70% large businesses and 57% medium businesses).
- Around one in seven businesses (14%) and one in five charities (22%) said they held personal data that was not protected by techniques such as anonymisation or encryption, suggesting that the majority do protect personal data (77% of businesses and 69% of charities).
- The majority of businesses (94%) and charities (80%) have undertaken key actions associated with at least one of the 10 Steps. The proportion of businesses undertaking actions associated with the 10 Steps has returned to previous levels following a decline last year (94% in 2023/2024, 89% in 2024/2025 and 94% in 2025/2026). The proportion of charities doing so remains in line with 2024/2025 (82%).
- Qualitative insights highlighted that recent high-profile cyber attacks in the media had moved the perception of risk from cyber attacks and breaches up the agenda within organisations. Despite this, staff training and awareness raising activities remained stable across businesses compared with last year (19% in both 2024/2025 and 2025/2026). There were signs of an increase among large businesses (76% in 2024/2025 to 84% in 2025/2026) but this did not represent a significant change.
- On the other hand, the proportion of charities running staff training and awareness raising activities has decreased since last year (17% in 2025/2026, down from 21% in 2024/2025), driven by a decline among low-income charities (13% in 2025/2026, down from 18% in 2024/2025).
- The proportion of businesses holding Cyber Essentials has increased since 2024/2025 (5% up from 3% in 2024/2025). This was driven by increases among large businesses (from 21% in 2024/2025 to 35% in

2025/2026) and among small businesses (from 5% in 2024/2025 to 12% in 2025/2026).

- Similarly to previous years, relatively few businesses or charities were taking steps to formally review the risks posed by their immediate suppliers and wider supply chain. 15% of businesses and 9% of charities said they reviewed the risks posed by their immediate suppliers.
- Around a third of businesses (31%) and a quarter of charities (25%) were either using AI, in the process of adopting it or actively considering using it. Of this group, around a quarter of businesses (24%) and charities (27%) reported having cyber security practices or processes in place to manage the risks from the use of AI technology.

3.1 Identifying, managing, and minimising cyber risks

Actions taken to identify risks
Organisations can take a range of actions to identify cyber security risks, including monitoring, risk assessment, audits, and testing. They are not necessarily expected to be doing all these things as the appropriate level of action depends on their own risk profiles.

Figure 3.1: Percentage of organisations that have carried out the following activities to identify cyber risks in the last 12 months

Change to table view

Activities	Businesses	Charities
Any of the listed activities	52%	38%
Used specific tools designed for security monitoring	32%	19%
Risk assessment covering cyber security risks	30%	27%
Tested staff (e.g. with mock phishing exercises)	22%	13%
Carried out a cyber security vulnerability audit	18%	10%
Penetration testing	13%	7%
Used or invested in threat intelligence	11%	6%

Bases: 2,112 businesses, 1,085 charities

Larger organisations were more likely to carry out these actions (91% of large businesses have carried out at least one of the actions, as have 81% of medium businesses and 80% of high-income charities), compared to 52% of businesses overall and 38% of charities overall.

The proportion of businesses deploying at least one of these activities has remained consistent with 2024/2025 (52% in 2025/2026 and 49% in 2024/2025). Businesses overall have seen no change in the proportion conducting risk assessments covering cyber security risks (30% in 2025/2026 and 29% in 2024/2025). Small businesses, however, have seen a significant decrease in those carrying out risk assessments covering cyber security (48% in 2024/2025 to 41% this year). This puts small businesses back in line with 2023/2024 levels (41%).

Charities carrying out at least one of the activities have also remained consistent with last year (38% in 2025/2026 and 42% in 2024/2025).

How organisations undertake audits and implement their findings
Among the 18% of businesses that undertook cyber security vulnerability audits, 28% carried out an internal audit only and 39% an external audit only. Three in ten businesses undertaking vulnerability audits (28%) carried out both internal and external audits.

The way that businesses undertook audits continues to be strongly linked to size:

- micro, small and medium businesses were most likely to solely use external contractors to undertake audits (36% micro businesses, 47% small businesses, and 44% medium businesses)
- large businesses, which typically had greater financial and personnel capacity, were more likely to state that audits have been undertaken both internally and externally (57%)

One in ten charities have carried out cyber security vulnerability audits (10%), however, contrary to the average business, the charities undertaking audits continued to be most likely do them solely on an internal basis only (45% compared to 27% of businesses). Around two in ten charities conducted both internal and external audits (20%) and one quarter carried out external only audits (25%).

A new question for 2025/2026 asked those that had carried out a cyber security vulnerability audit what was included in the audits. The most common elements to be covered in the audits included:

- Whether there was a cyber security strategy in place (around three quarters of businesses (77%) and charities (74%))

- Whether all board members were actively involved in discussions of cyber security in their audit (two thirds of businesses (65%) and three in five charities (60%))
- Whether cyber security was incorporated into the broader organisational governance structure (three in five businesses (62%) and two in three charities (67%)

Cyber security considerations when purchasing software
Businesses were also asked about the role that cyber security considerations played when purchasing new software. As shown in Figure 3.2, around a fifth of businesses (22%) and 17% of charities considered cyber security to a large extent when purchasing software. For the bulk of businesses and charities, however, it was not a major concern (38% of businesses and 31% of charities) and for sizeable minority (12% of businesses and 17% of charities) it was not a consideration at all.

Large businesses were significantly more likely to consider cyber security to a large extent when purchasing software (69%), whereas micro businesses were more likely to not consider it at all (13%). The proportion of medium businesses that considered cyber security to a large extent when purchasing software has significantly increased this year, up to 54% from 43% in 2024/2025. The proportion of high-income charities that considered cyber security to a large extent when purchasing software has also increased, from 37% in 2024/2025 to 45% in 2025/2026.

Figure 3.2: Role of cyber security considerations when purchasing new software

Change to table view

Organisation type	% a large extent	% to some extent, but it is not a major concern	% not a major concern, purchase from established companies	% to no extent, do not consider	% Don't know	Tota
Businesses	22	20	38	12	7	
Charities	17	18	31	17	17	

Bases: 2,112 businesses, 1,085 charities
Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

3.2 Cyber security strategies

Larger organisations, including medium and large businesses and high-income charities were asked if they had a formal cyber security strategy in place, a document underpinning all policies and processes relating to cyber security. The majority of large businesses (74%) had one in place. As shown in Figure 3.3, fewer medium businesses had a formal cyber security strategy (57%).

The proportion of both medium and large businesses that had a strategy has remained consistent with 2024/2025 (57% medium and 70% large).

Figure 3.3 : Percentage of organisations that have a formal cyber security strategy in place

Change to table view

Organisation type	
Medium businesses	57%
Large businesses	74%
High-income charities	44%

Bases: 296 medium businesses,155 large businesses, 335 charities

Among the larger organisations that had a cyber security strategy in place, around eight in ten businesses (83%) and three-quarters of charities (77%) reported that this had been reviewed by senior executives or trustees within the last 12 months.

3.3 Insurance against cyber security breaches

Which organisations are insured?
Almost half of businesses (47%) and a third of charities (35%) reported being insured against cyber security risks in some way. In most cases, as Figure 3.4 shows, organisations' cyber security insurance was part of a wider insurance policy: only 10% of businesses and 5% of charities had a specific cyber security insurance policy. Larger businesses (24% of medium

businesses and 32% of large businesses) and high-income charities (20%) were more likely to have a specific policy in place.

As in previous years, small and medium businesses were more likely than businesses overall (47%) to have some form of cyber insurance (55% small businesses and 61% medium businesses). This could be because small and medium businesses were more likely to be able to afford insurance than micro businesses but may not have had the skills or tools to be able to address all cyber security risks internally like larger businesses.

It is worth noting the high level of uncertainty that remained at this question, in line with previous years. One in five businesses (22%) and 13% of charities did not know if they had any form of cyber security insurance, despite the survey being carried out with the individual identified by the organisation as having the most responsibility for cyber security.

Figure 3.4 : Percentage of organisations that have the following types of insurance against cyber security risks

Change to table view

Organisation	Cyber security cover as part of a wider insurance policy	A specific cyber security insurance policy
Micro businesses	37%	8%
Small businesses	40%	15%
Medium businesses	36%	24%
Large businesses	22%	32%
Businesses overall	37%	10%
Charities overall	31%	5%

Bases: Split-sample half A: 580 micro businesses, 241 small businesses,154 medium businesses, 76 large businesses,1,051 businesses, 530 charities

Trends over time

Compared to the 2023/2024 and 2024/2025 survey, the proportion of businesses with some form of insurance has remained broadly consistent (43% in 2023/2024, 45% in 2024/2025 and 47% in 2025/2026).

The proportion of charities overall with some form of insurance has remained consistent (34% in both 2023/2024 and 2024/2025, and 35% in 2025/2026). However, the proportion of high-income charities that have some form of insurance has significantly increased since last year (64% in 2024/2025 to 75% in 2025/2026). This was due to an increase in those that have cyber security cover as part of a broader insurance policy (41% in 2024/2025 to 55% 2025/2026).

Organisations who did not have any cyber insurance were also asked why they did not have it. As shown in Figure 3.5, lack of awareness of cyber insurance (39% of businesses and 24% of charities) and it not being a budgetary priority (34% of businesses and 34% of charities) were the two largest barriers to holding a cyber insurance policy.

Figure 3.5 : Reasons why organisations are not covered by a cyber insurance policy

Change to table view

Reason	Businesses	Charities
Not aware of cyber insurance	39%	24%
Not a budgetary priority	34%	34%
Leadership not interested in cyber insurance	27%	24%
Too expensive	19%	16%
Not needed / no relevant risk perceived	13%	16%
Limited IT infrastructure	8%	15%
Coverage not broad enough	8%	8%
Don’t know	1%	3%

Bases: Those that don’t have a cyber insurance policy: 267 businesses, 213 charities

Qualitative insights on cyber insurance
When asked about the factors considered in purchasing cyber insurance, a common theme was having return on investment. Some organisations

perceived cyber insurance as an investment that was worth it. Generally, there seemed to be an apparent uptake in new cyber insurance policies in the 12 months prior to the survey, or increased cover from existing cyber insurance policies.

> "We have cyber insurance now, that we took out 12 months ago. Mainly because I'm just on my own and it was felt that it would be nice for me to have some professional advice and guidance. Obviously there's also now the concerns wrapped around GDPR and things like that. So it was deemed quite useful and worth the policy premium." **Medium business, Wholesale/retail**

Organisations that did believe cyber insurance was worth the investment often highly valued the insurance provider as a source of advice and support, rather than just for the financial coverage. This can also be linked to the awareness of high-profile cyber attacks and the cost of these attacks.

> "Yes, we've got cyber insurance. The growing cost of attacks and ransomware is why we've got it. It is so important to have that level of cover and expertise as well, financial guidance, comms, legal assistance." **Large business, Real estate**

However, not all organisations thought that the investment in insurance was worth it. One large business described an investment in their own recovery speed, prioritising their systems and processes rather than obtaining cyber insurance.

> "It doesn't make sense to have it, we are investing in recovery speed. If we can recover and get back up and running quickly, it is better than getting an insurance lump of money afterwards. " **Large business, Transport and storage**

3.4 Technical cyber security controls

Each year, organisations are asked whether they have a range of technical rules and controls in place to help minimise the risk of cyber security breaches or attacks. The full list is shown in Figure 3.6. Many of these are basic good practice controls taken from government guidance such as the 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps) or the requirements for Cyber Essentials (https://www.ncsc.gov.uk/cyberessentials/overview) certification.

A clear majority of businesses and charities had a broad range of basic rules and controls in place. The most frequently deployed rules or controls involved updated malware protection, cloud backups, passwords, network firewalls and restricted admin rights, each administered by at least two-thirds of businesses. The least common rules and controls were data backups, two-factor authentication (2FA), rules for personal data storage, separated Wi-Fi networks, use of Virtual Private Networks (VPNs), applying software updates, and user monitoring (with exact percentages included in Figure 3.6).

Figure 3.6 : Percentage of organisations that have the following rules or controls in place

Change to table view

Rules or controls	Businesses	Charities
Up-to-date malware protection	81%	63%
Backing up data securely via a cloud service	74%	57%
A password policy that ensures that users set strong passwords	74%	56%
Firewalls that cover the entire IT network, as well as individual devices	74%	45%
Restricting IT admin and access rights to specific users	73%	65%
Only allowing access via organisation-owned devices	66%	35%
Security controls on organisation-owned devices (e.g. laptops)	61%	42%
An agreed process for staff to follow with fraudulent emails or websites	58%	36%
Rules for storing and moving personal data securely	51%	47%
Backing up data securely via other means	48%	38%
Any Two-Factor Authentication (2FA) for networks/applications	47%	38%

Rules or controls	Businesses	Charities
Separate Wi-Fi networks for staff and visitors	38%	25%
A virtual private network, or VPN, for staff connecting remotely	36%	17%
A policy to apply software security updates within 14 days	34%	20%
Monitoring of user activity	33%	28%

Bases: 2,112 businesses, 1,085 charities

Medium and large businesses were more likely than average to have each of these technical rules and controls in place. Specifically, across large businesses, over nine in ten have adopted each of the following:

- password policies (96%)
- restricting admin rights (96%)
- data backups, either via the cloud or other means (90%)
- security controls on their devices (91%)
- up-to-date malware protection (93%)
- network firewalls (93%)
- requirements for two-factor authentication (90%)
- an agreed process for staff to follow when they identify a fraudulent email (94%)

Trends over time
Compared to 2024/2025, the deployment of controls and procedures has remained stable for several procedures, but has increased slightly for some controls among businesses:

- using up-to-date malware protection (up from 77% in 2024/2025 to 81% in 2025/2026)
- restricting admin rights (up from 68% in 2024/2025 to 73% in 2025/2026)
- only allowing access via company-owned devices (up from 61% in 2024/2025 to 66% in 2025/2026)
- separate Wi-Fi networks for staff and visitors (up from 33% in 2024/2025 to 38% in 2025/2026)
- backing up data securely via a cloud service (up from 71% in 2024/2025 to 74% in 2025/2026)

- a virtual private network, or VPN, for staff connecting remotely (up from 31% in 2024/2025 to 36% in 2025/2026)
- requirements for two-factor authentication (up from 40% in 2024/2025 to 47% in 2025/2026)

For some of these rules, these increases reverse the decline observed in 2024/2025, returning to 2023/2024 levels.

These uplifts were largely due to shifts among micro businesses towards incorporating more rules, such as only allowing access via company-owned devices (up from 58% in 2024/2025 to 64% in 2025/2026) and requiring two-factor authentication (up from 35% in 2024/2025 to 43% in 2025/2026).

Whilst large businesses remained in line with where they were in 2024/2025 across most measures, there was a significant decline in the proportion of large businesses that have a separate Wi-Fi network for staff and visitors (93% in 2024/2025 and 85% in 2025/2026).

The proportion of charities who deployed these various controls and procedures has also remained relatively consistent since 2024/2025.

3.5 Staff training and awareness raising

This survey does not explore cyber security skills and training in detail, given that there was another annual government study dealing with this topic, the Cyber security skills series (https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024). Nevertheless, staff training is an important aspect of the 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/user-education-and-awareness) guidance, so we continue to estimate the proportion of organisations that have undertaken training or awareness raising activities around cyber security in the past year.

Results (Figure 3.7) show that in the last 12 months, around a fifth of businesses (19%) and charities (17%) have provided some form of staff training. Over half of all medium businesses (54%), around four in five large businesses (84%) and around half of high-income charities (49%) provided training.

Figure 3.7 : Percentage of organisations that have had training or awareness raising sessions on cyber security in the last 12 months

Change to table view

Organisation type	
Micro businesses	14%
Small businesses	33%
Medium businesses	54%
Large businesses	84%
Businesses overall	19%
Charities overall	17%

Bases: 1,154 micro businesses; 507 small businesses; 296 medium businesses; 155 large businesses; 2,112 businesses overall; 1,085 charities overall

Trends over time
Qualitative insights highlighted that recent high-profile cyber attacks in the media had moved the risk of cyber attacks and breaches up the agenda within organisations. Despite this, staff training and awareness raising activities remained stable across businesses compared with last year (19% in both 2024/2025 and 2025/2026). There were signs of an increase among large businesses (76% in 2024/2025 to 84% in 2025/2026) but this did not represent a significant change. For charities, the proportion running training has decreased since last year (17% in 2025/2026, down from 21% in 2024/2025), which could be due to a decline among low-income charities (13% in 2025/2026, down from 18% in 2024/2025).

3.6 Responsibility for cyber security

The job titles of those completing the survey, who were identified by their organisation as being the individual most responsible for cyber security, provided an insight as to the likely seniority and influence of these individuals.

These results do not necessarily show the definitive proportion of organisations that have, for example, a Chief Information Officer (CIO) or Chief Information Security Officer (CISO), they simply show how many of them completed the survey. In organisations with these functions, we may

have been directed to another senior individual with more day-to-day responsibility for cyber security, such as a senior IT colleague.

Generally, the larger the organisation, the more specific the job title of the individual covering cyber security matters. The findings outlined here were all in line with the previous year (2024):

- in micro businesses, it was most likely to be a business owner (16%), Chief Executive (22%), or another senior management role (18%). Very few micro businesses had someone specifically in an IT-role looking after cyber security matters (3%)
- in small businesses, as with micro businesses, very few had someone specifically in an IT-role looking after cyber security. The most common job roles were general office managers (26%), those with another (unspecified) senior management role (18%) or Chief Executives (14%)
- in four in ten large businesses, it was either the IT director (26%) or an IT manager, technician or administrator (13%) looking after cyber security. The respective figures for medium sized businesses were 13% and 14%
- in two in three charities (35%), a trustee performed this function. Compared to charities overall, for high-income charities it was more likely to be completed by those in a senior management role (16%), general or office managers (17%) or Chief Executives (11%)

3.7 Outsourcing of cyber security functions

Around half of businesses (48%) and a quarter of charities (25%) had an external cyber security provider. These overall figures are broadly consistent with those recorded in the previous four years of the survey.

As Figure 3.8 shows, outsourcing of cyber security was substantially higher among small (64%) and medium (70%) businesses, as opposed to micro (44%) and large (42%) businesses. This pattern has also been evidenced in previous years. It was possible that large businesses were relying more on internal cyber security expertise than on outsourcing, while micro businesses perhaps could not afford to recruit specialists to the same extent. However, the proportion of micro businesses with an external cyber security provider was growing, (39% in 2024/2025, increased to 44% in 2025/2026).

Figure 3.8 : Percentage of organisations that have an external cyber security provider

Change to table view

Organisation type	
Micro businesses	44%
Small businesses	64%
Medium businesses	70%
Large businesses	42%
Businesses overall	48%
Charities overall	25%

Bases: 1,154 micro businesses; 507 small businesses; 296 medium businesses; 155 large businesses; 2,112 businesses overall; 1,085 charities overall

3.8 Cyber security policies and other documentation

Do organisations formally document their approaches?
A third of businesses (36%) and charities (33%) reported having formal cyber security policies in place. To note, these may be part of a wider policy within the organisation, such as the IT policy. A similar proportion of businesses (33%), and a smaller proportion of charities (20%) had a business continuity plan that covered cyber security.

Figure 3.9 shows strong differences by size, with the majority of medium and large businesses having each form of documentation. Reversing the increases observed last year, small businesses have seen significant decreases in both having a formal policy covering cyber security risks (down from 59% in 2024/2025 to 52% in 2025/2026) and having a business continuity plan that covered cyber security (down from 53% in 2024/2025 to 44% in 2025/2026).

Figure 3.9 : Percentage of organisations that have a cyber security policy or business continuity plan

Change to table view

Organisation type	A formal policy or policies covering cyber security risks	A business continuity plan that covers cyber security
Micro businesses	31%	29%
Small businesses	52%	44%
Medium businesses	75%	73%
Large businesses	89%	85%
Businesses overall	36%	33%
Charities overall	33%	20%

Bases: 1,154 micro businesses; 507 small businesses; 296 medium businesses; 155 large businesses; 2,112 businesses overall; 1,085 charities overall

When were policies last reviewed?
Of businesses and charities that had cyber security policies in place, the majority had reviewed them within the last 12 months (77% businesses and 72% charities). However, as detailed in Figure 3.10, this did leave 14% of businesses and 17% of charities who had reviewed their cyber security policies between one and two years ago and a minority (3% of businesses and 6% of charities) who had reviewed them more than two years ago.

For businesses and charities, the proportion updating or reviewing their cyber security policies remained in line with recent years.

Figure 3.10 : When organisations last created, updated, or reviewed their cyber security policies or documentation to make sure they were up to date

Change to table view

Organisation type	% Within the last 3 months	% Between 3 months and 6 months ago	% Between 6 months and 12 months ago	% Between 1 and 2 years ago	% More than 2 years ago	Don't know
Businesses	23	19	35	14	3	7
Charities	24	16	33	17	6	5

Bases: Those with cyber security policies in place: 985 businesses, 492 charities
Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

What is covered in cyber security policies?
As Figure 3.11 indicates, cyber security policies tended to cover a range of topics. The aspects most often covered were data storage (84% businesses and 85% charities) and the appropriate use of the organisation's IT devices (84% businesses and 76% charities).

Figure 3.11 : Percentage of organisations with cyber security policies that have the following features in their cyber security policies

Change to table view

Features	Businesses	Charities
How data is supposed to be stored	84%	85%
What staff are permitted to do on organisation's IT devices	84%	76%
Use of cloud computing	71%	60%
Remote or mobile working	68%	69%
Use of network-connected devices	66%	55%
What can be stored on removable devices (e.g. USB sticks)	64%	62%
Digital Service Providers such as cloud services	62%	51%

Features	Businesses	Charities
Use of personally-owned devices for business activities	58%	65%

Bases: Those with cyber security policies in place: 985 businesses, 492 charities

3.9 Cyber accreditations and government initiatives

This section looks at both government and external cyber accreditations and initiatives. It looks at which organisations adhere to specific accreditations. It then combines some of the results regarding individual actions and controls covered earlier in this chapter, to provide estimates of how many businesses and charities are fulfilling the range of requirements laid out in two government initiatives Cyber Essentials (https://www.ncsc.gov.uk/cyberessentials/overview) and the 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security).

Cyber Essentials
The government-endorsed Cyber Essentials scheme enables organisations to be independently certified for having implemented a good-practice standard in cyber security, which protects against the most common cyber-attacks. Specifically, it requires them to enact basic technical controls across five areas (https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=cyber%20essentials&sort=date%2Bdesc):

- boundary firewalls and internet gateways
- secure configurations
- user access controls
- malware protection
- patch management (i.e. applying software updates)

Chapter 2 highlighted that overall, there was low, although growing, awareness of Cyber Essentials among businesses (17%) and charities (16%). Despite this lack of awareness, a slightly higher proportion of businesses did have technical controls in these five areas.

The survey asked questions which corresponded to the five areas.[footnote 9] In total, 24% of businesses and 13% of charities reported having technical controls in all five areas. As might be expected, this was considerably higher for medium businesses (51%), large businesses (70%) and high-income charities (44%).

The overall proportions were still lower than in 2020/2021, when 29% of businesses and 20% of charities had technical controls in place in all five Cyber Essentials areas, but were broadly in line with 2024/2025, where 21% of businesses and 12% of charities had controls in all five areas.

Organisations were also asked if they recalled adhering to either the Cyber Essentials or Cyber Essentials Plus standards. Both require organisations to implement cyber security measures in the same five areas, but the latter included an external technical assessment. This year's results show that 5% of businesses and 3% of charities reported adhering to Cyber Essentials. For businesses, this was a significant increase from 2024/2025, where 3% reported adhering to Cyber Essentials, whereas for charities, this was consistent with 2024/2025 (also 3%). Just 2% of businesses and 1% of charities said they adhered to the Cyber Essentials Plus standard. Among large businesses, accreditations were more common, with 35% holding Cyber Essentials and 12% achieving Cyber Essentials Plus. For Cyber Essentials, this was a significant increase from 2024/2025, where 21% reported adhering to it. This continued to indicate that some organisations, especially medium and large businesses, were potentially already meeting the Cyber Essentials standard, but not seeking certification.

It is worth noting the high level of uncertainty towards this question. Two in five businesses (18%) and around one in six charities (16%) did not know if their organisation adhered to either Cyber Essentials, Cyber Essentials Plus or ISO 27001, despite the survey being carried out with the individual identified by the organisation as having most responsibility for cyber security.

Qualitative insights on the motivations behind seeking accreditation
In the qualitative interviews, the uptake of Cyber Essentials and Cyber Essentials Plus was commonplace. The associated benefits of Cyber Essentials and Cyber Essentials Plus were widely recognised. The broad reasons for its uptake included procurement, client and business strategy incentives, practical cyber security incentives such as identifying gaps for threats and insurance and cost-benefit incentives.

In some cases, reasons for obtaining or maintaining Cyber Essentials Plus were sector specific or aligned with business strategy. For instance, a small business in the information and communication sector identified clients were requesting Cyber Essentials, prompting investigation into becoming accredited by the business.

> "[Cyber Essentials] is something I need to investigate purely because clients are asking for it." **Small business, Information and communication**

Some organisations mentioned that having Cyber Essentials was useful as a measure of their cyber security posture. For example, one medium business thought the process of attaining Cyber Essential Plus was valuable to identify any cyber security gaps that otherwise might go unnoticed. Another business thought the structure was helpful for smaller businesses to follow because it allowed them to implement important security measures without impacting the day-to-day running of the business too much.

> "I think the Cyber Essentials approach… I think that's an excellent overall structure for protecting a smallish business. The way the National Cyber Security Centre describe it, it's the equivalent of making sure your door's locked when you leave the house. We take that framework and use it to look at how we do things. You can take it too far, make measures which would make us less competitive, make it more difficult for people to do their jobs. We don't want to do that. On the other hand, we do have to make sure that we have done the basic things necessary to be a hard target. That's the trick." **Medium business, Transport or storage**

Some organisations also mentioned needing Cyber Essentials or Cyber Essentials Plus to be able to take out an affordable cyber insurance policy.

> "If you don't have at least Cyber Essentials, then insurance will be prohibitively expensive. The very fact of having Cyber Essentials, essentially if nothing else, it is a sign that you are taking things seriously." **Charity, England and Wales**

In contrast, some organisations highlighted the accreditations could be burdensome to obtain, with legacy, technology and organisation type constraints limiting their applicability in some cases. One large manufacturing business noted that their old older software did not comply, which was a barrier to obtaining accreditation.

> "As a manufacturer, our machines rely on old software and that would not comply with Cyber Essentials." **Large business, Manufacturing**

In addition, one charity described how their organisational structure and systems did not transfer easily to the Cyber Essentials frameworks, and therefore these frameworks were less pragmatic for the charity. They adhered loosely to Cyber Essentials but did not see the value in gaining the accreditation. The Centre for Internet Security guidance was seen to be more pragmatic for their organisation compared to Cyber Essentials. Despite this, the charity considered adhering to Cyber Essentials Plus

because it was becoming more common for cyber insurance providers to request Cyber Essentials Plus. This could result in a financial gain, which makes adherence worth the cost. Another charity also highlighted the positive effect of standards and accreditations on the financial cost of cyber insurance.

> "I've never found Cyber Essentials as a standard very useful. Cyber Essentials Plus, I think, is gradually gaining traction within things like cyber insurance. So simply by having the accreditation I'm starting to consider it more as a means to an end rather than because it's particularly useful." **Charity, Education**

10 Steps to Cyber Security

The 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps) is government guidance that breaks down the task of managing cyber risk across an organisation into 10 key components. It is intended to provide a broad set of areas organisations should address to have a good corporate approach to cyber security. It is not, however, an expectation that organisations fully apply all the 10 Steps and this will depend on each organisation's ways of working.

These steps have been mapped to several specific questions in the survey (in Table 3.1), bringing together findings that have been individually covered across the rest of this chapter. This is not a perfect mapping as some of the steps are overlapping and require organisations to undertake action in the same areas. However, it does provide an indication of whether organisations have taken relevant actions on each Step. This is regardless of whether they are actually aware of the 10 Steps guidance (covered earlier in Section 2.3).

As a remapping exercise took place in 2022/2023, the 2025/2026 results for the 10 Steps to Cyber Security are only comparable to results since 2022/2023.

The 10 Steps are actions that all organisations can take, but the guidance was specifically aimed at medium to large organisations. As such, we have shown the results for medium and large businesses, as well as businesses overall, in Table 3.1.

Table 3.1: Percentage of organisations undertaking key actions in each of the 10 Steps areas

Step	Step description	Businesses	Medium businesses	Large businesses	Chari
1	**Risk management**	30%	62%	72%	27%

Step	Step description	Businesses	Medium businesses	Large businesses	Chari
	organisations have undertaken a cyber security risk assessment				
2	**Engagement and training** organisations have carried out staff training or awareness raising activities	19%	54%	84%	17%
3	**Asset management** organisations have a list of critical assets	29%	59%	70%	29%
4	**Architecture and configuration** organisations have at least three of the following technical rules or controls: up-to-date malware protection, network firewalls, restricted IT admin and access rights, security controls on organisation-owned devices, only allowing access via organisation-owned devices, separate Wi-Fi networks for	81%	97%	96%	58%

Step	Step description	Businesses	Medium businesses	Large businesses	Chari
	staff and visitors, specific rules for personal data storage and transfer, or a VPN				
5	**Vulnerability management** organisations have policy to apply software security updates within 14 days	34%	56%	73%	20%
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	47%	79%	90%	38%
7	**Data security** organisations have cloud backups or other kinds of backups	88%	95%	90%	72%
8	**Logging and monitoring** organisations fulfil at least one of the following	48%	80%	91%	36%

Step	Step description	Businesses	Medium businesses	Large businesses	Chari
	criteria: using specific tools designed for security monitoring, such as Intrusion Detection Systems, or doing any monitoring of user activity				
9	**Incident management** organisations have a formal incident response plan, or at least three of the following: written guidance on who to notify of breaches, roles or responsibilities assigned to specific individuals during or after an incident, external communications and public engagement plans, guidance around when to report incidents externally	32%	64%	83%	25%
10	**Supply chain security** organisations monitor risks	16%	31%	51%	10%

Step	Step description	Businesses	Medium businesses	Large businesses	Chari
	from suppliers or their wider supply chain				

Significant changes from last year include:

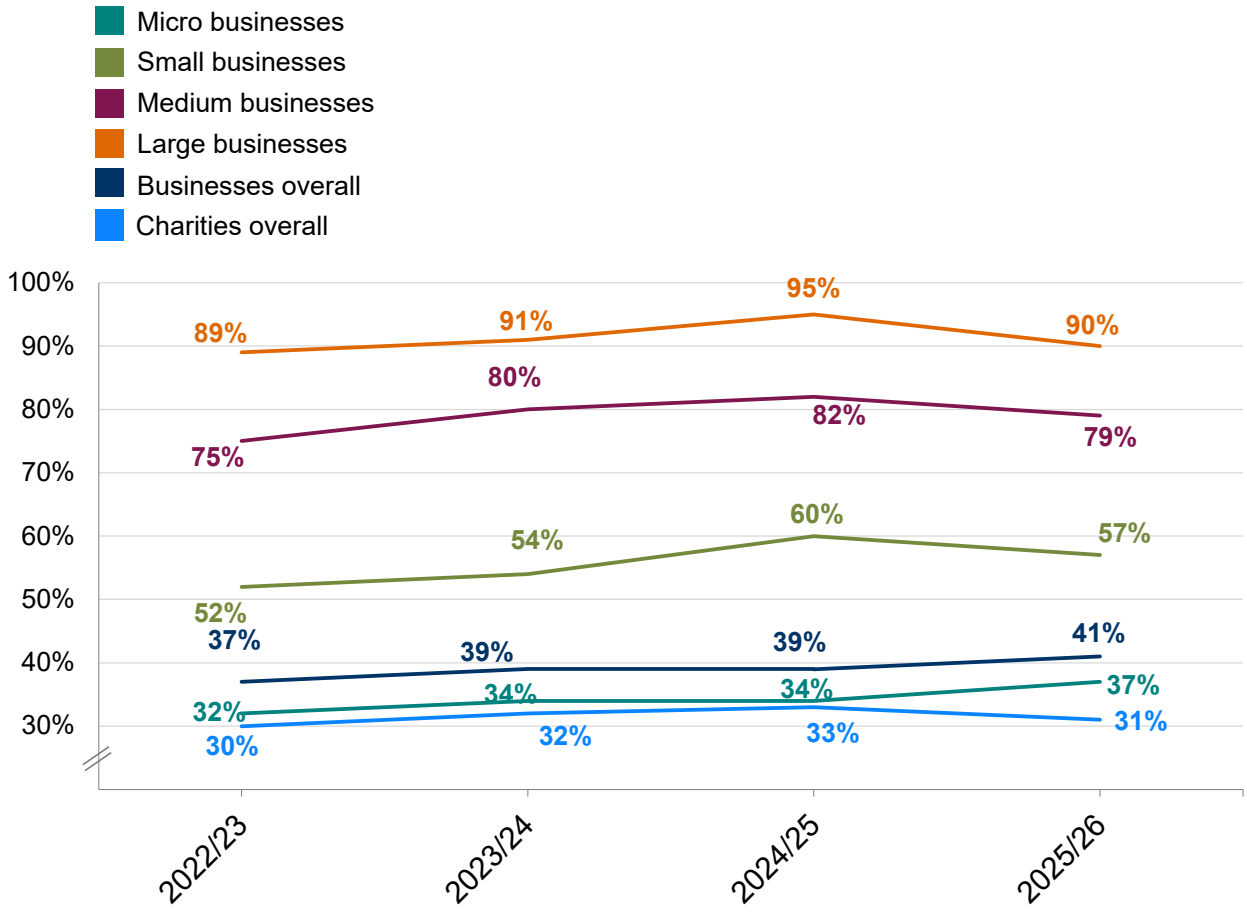
- The proportion of businesses undertaking architecture and configuration has increased to 81% this year, from 75% in 2024/2025
- The proportion of businesses undertaking identity and access management has increased to 47% this year, from 40% in 2024/2025
- The proportion of businesses undertaking data security has increased to 88% this year, from 83% in 2024/2025

The majority of businesses (94%) and charities (80%) had undertaken key actions associated with at least one of the 10 Steps. The proportion of charities doing so remained in line with 2024/2025 (82%), however, the proportion of businesses has returned to 2023/2024 levels following the decline in 2024/2025 (94% in 2023/2024, 89% in 2024/2025 and 94% in 2025/2026).

Two-fifths of businesses (41%) and a third of charities (31%) had taken action on 5 or more of the 10 Steps in 2025/2026, as Figure 3.12 shows. This was also much higher in large businesses, where 90% had progressed at least 5 of these Steps.

A minority of businesses (3%) had undertaken action in all of the 10 Steps, but this was higher among medium (13%) and large (30%) businesses.

Figure 3.12: Percentage of organisations that have undertaken action in 5 or more of the 10 Steps guidance areas, over time



Bases: 2,000+ businesses per year; 1,000+ micro businesses per year; 400+ small businesses per year; 260+ medium businesses per year; 170+ large businesses per year; 1,000+ charities per year

Results have remained consistent for businesses and charities at the overall level, as well as by business size.

3.10 Supply chain risk management and supplier standards

Reviewing supplier risks
Suppliers can pose various risks to an organisation's cyber security, for example:

- third-party access to an organisation's systems
- suppliers storing the personal data or intellectual property of a client organisation
- phishing attacks, viruses or other malware originating from suppliers

Despite this, relatively few businesses or charities were taking steps to formally review the risks posed by their immediate suppliers and wider supply chain. Just over one in ten businesses said they reviewed the risks

posed by their immediate suppliers (15%) and around one in twenty were looking at their wider supply chain (6%). Among charities, the respective figures were slightly lower (9% looked at their immediate suppliers and 4% at their wider supply chain).

As Figure 3.13 shows, there was extensive variation by size of organisation which was consistent with previous years. Possibly reflecting a more complex supply chain, around a third of medium businesses (30%) and nearly half of large businesses (48%) reviewed the cyber security risks posed by their immediate suppliers, in comparison to 12% of micro businesses and 22% of small businesses. It was still relatively rare for medium and large businesses to review their wider supply chain (13% and 24% respectively do so).

The proportion of charities overall reviewing immediate supplier risks (9% in 2023/2024, 2024/2025 and 2025/2026) has remained consistent, but there has been a significant increase amongst high-income charities (from 21% in 2024/2025 to 31% this year). This follows a decline in 2024/2025 (from 36% in 2023/2024). Additionally, the proportion of high-income charities that had reviewed their wider supply chains has started to recover following the drop in 2024/2025 (15% in 2023/2024, 6% in 2024/2025 and 11% in 2025/2026).

Figure 3.13 : Percentage of organisations that have carried out work to formally review the potential cyber security risks presented by the following groups of suppliers

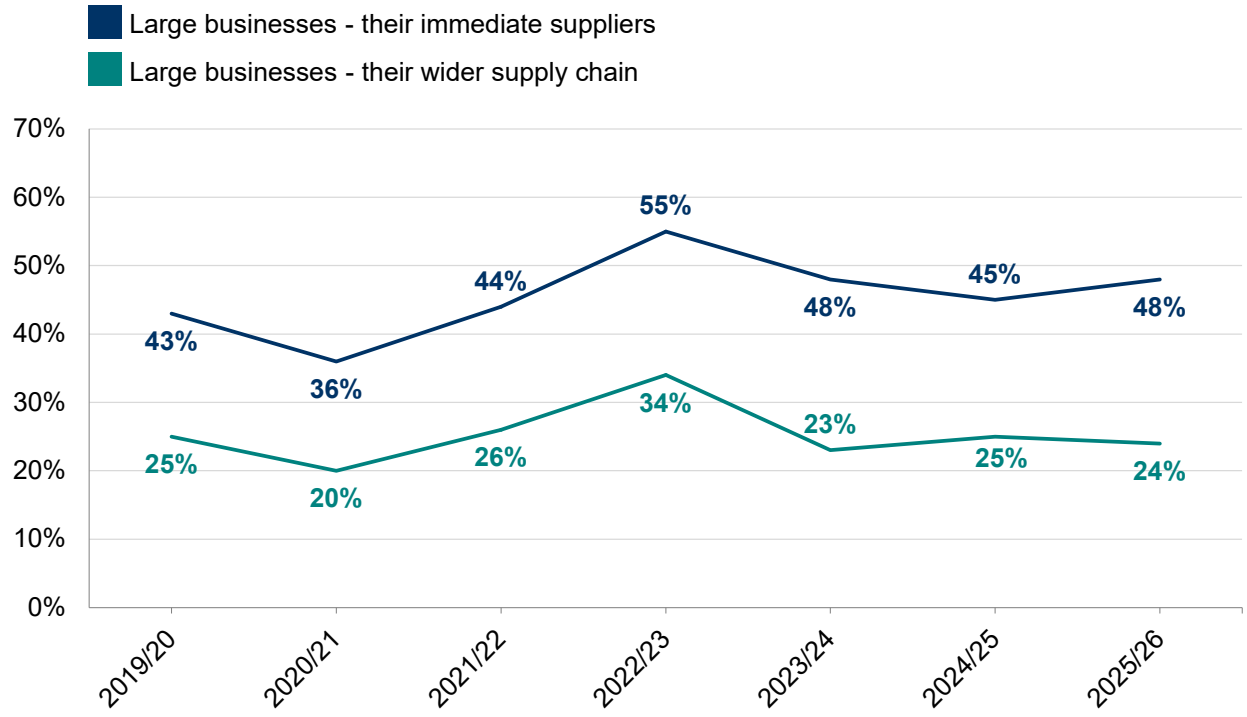
Change to table view

Business size	Their immediate suppliers	Their wider supply chain
Micro businesses	12%	5%
Small businesses	22%	10%
Medium businesses	30%	13%
Large businesses	48%	24%
Businesses overall	15%	6%
Charities overall	9%	4%

Bases: 2,112 businesses, 1,085 charities, 1,154 micro businesses, 507 small businesses, 296 medium businesses, 155 large businesses

Trends over time
This question has been asked since the 2019/2020 study and remains relatively stable at the overall level. Among large businesses, as outlined in Figure 3.14, the proportion saying they reviewed the risks posed by their immediate suppliers (48%) and wider supply chain (24%) has remained stable over the last few years, despite a spike 2022/2023.

Figure 3.14: Percentage of large businesses over time that have carried out work to formally review the potential cyber security risks presented by the following groups of suppliers



bases (per year): 100+ large businesses.

Very few organisations required their suppliers to be certified via standards or accreditations. Only 11% of businesses and 7% of charities required their suppliers to be certified with any standards or accreditations. This rose to one in five high-income charities (20%) and two in five large businesses (41%), which was significantly higher than in 2024/2025 (21%).

A smaller proportion of businesses (3%) and charities (3%) required their suppliers to be accredited with Cyber Essentials specifically. This rose to one in ten high-income charities (10%) and around a quarter of large businesses (26%), significantly higher than in 2024/2025 (10%).

Qualitative insights on broad supply chain risks
Knowledge or understanding of supply chain risk continued to be a challenge for businesses and charities, however, some organisations reported that supply chain risk management was increasingly important to customers. Supply chain management included activities such as checking suppliers had accreditations such as Cyber Essentials, issuing suppliers

with tailored cyber security questionnaires and checking the way suppliers stored or processed sensitive data.

> “In the last 12 months we’ve mandated that any new suppliers need to have Cyber Essentials Plus. They need to have the plus because that means there are trained auditors that they’ve had on site to test their underlying infrastructure and that’s so important it’s not just self-reported.” **Large business, Real estate**

Size and sector appeared to be drivers of proactive supply chain risk management. For example, in more highly regulated sectors like healthcare, where regulations were perceived to be stringent, organisations were more likely to take a more formal approach to supply chain risk management.

> “We’re very comfortable with our suppliers because we go through so much due diligence with them and we make sure that every year we are getting updated.” **Charity, Healthcare**

However, a number of smaller businesses and charities outside of highly regulated industries tended to avoid supply chain risk management altogether. Organisations generally mentioned that purchasing software either had little or no cyber security considerations. One medium-sized business explained that a Customer Relationship Management (CRM) solution they worked with did not meet the cyber expectations they outlined before working with them, potentially leaving them exposed.

> “We’ve recently moved onto a new CRM solution and this CRM solution doesn’t even support multi factor authentication. Which I mentioned at the beginning when we were implementing the solution, but it still didn’t stop us adopting it. So, from my perspective that was a little bit disappointing and could be improved.” **Medium business, Wholesale/Retail**

Managed Service Providers (MSPs) were commonly used by organisations, especially smaller organisations, often for reasons around capacity constraints. Organisations with smaller teams highlighted 24/7 access to MSPs as a significant advantage for cyber defence. This advantage stemmed from the MSP’s ability to monitor or take proactive actions outside regular work hours, compared to cyber staff that were in-house. Sometimes MSPs pushed organisations to be more robust through leading penetration testing, gap analyses and encouraging Cyber Essentials accreditation.

> “Our MSP will generally bring any issues to my attention first. We’ve also got recently brought in a service with them where they will search for vulnerabilities and they will fix them.” **Medium business, Construction**

3.11 Artificial Intelligence (AI) adoption and cyber security risk management

A new section added in 2025/2026 focused on the use of AI by organisations. As outlined in Figure 3.15, around one in five businesses (21%) and charities (18%) reported adopting some AI tools in the organisation. Almost half of businesses (45%) and almost six in ten charities (57%) reported AI not being relevant to their organisation.

Figure 3.15 : Use of Artificial Intelligence (AI) within organisations

Change to table view

Organisation type	% Adopted some AI tools	% In the process of adopting AI	% Actively considering adopting AI at some point	% May adopt AI, but no plans to do so	% AI not relevant to organisatio
Businesses	21	4	6	19	45
Charities	18	3	4	15	57

Bases: 2,112 businesses, 1,085 charities

Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

Medium and large businesses were more likely to have adopted some AI tools in their organisation (39% of medium businesses and 45% of large businesses). Likewise, high-income charities were also more likely to have adopted some AI tools in their organisation (32%, compared to 18% on average).

Of those who used AI, were in the process of adopting it or who were considering using it, around a quarter of businesses (24%) and charities (27%) reported having security practices or processes in place to manage the risks from the use of AI technology. A further two in five organisations reported planning to implement these processes in the next 12 months (38% of businesses and 37% of charities). Just under a third of those using or considering using AI reported having no plans to implement security practices to manage the risks of AI (31% of businesses and 28% of charities).

Qualitative insights on Artificial Intelligence (AI)
Whilst AI adoption among organisations was broadly on the rise in the past 12 months, the use of AI tools in cyber security resilience varied greatly between organisations.

Organisations that seemed more open to using AI tended to mention that these were very recent considerations. The capability and trust levels between using different AI companies highlighted how AI could be used. For example, one charity mentioned they used a closed-source AI tool as they had control over the data in-house rather than open-source AI.

> "We've changed recently to be more open about using AI, but we use closed-source AI… to ensure that the team uses that and it's sort of held internally rather than it's suddenly going to open-source AI." **Charity, England and Wales**

When prompted, most organisations stated they did not use AI as a form of cyber defence. However, some organisations seemed open to using AI security products if they could trust it.

> "If somebody brought out an AI security product, then I'd look at it. I'd need the equivalent of an [Accountant qualification] for AI before I'd even let it go anywhere near our spreadsheets." **Small business, Administration**

The ability to trust and control data within AI products was a central theme to most discussions. Organisations that were open to using AI often caveated that they were using it, or would use it, because it offered organisational control and data transparency. Themes of trust, cost and return on investment were particularly related to timescales of using AI. Some organisations mentioned that staff were interested in using the products as soon as possible, but the cyber security teams had to be vigilant and careful about the risks.

> “We are not about to rush into [using AI] because we want to get that right, it’s a slow burn process… The only AI that we have running at the moment is a chatbot on our website which is very restricted. It’s like talking to our website.” **Small business, Utilities or production**

Another barrier for AI use appeared to be regulation. Some organisations that were hesitant about AI tools were waiting for stronger, up to date regulation before exploring the use of AI.

> “The government needs to establish a standard [AI] framework.” **Large business, Travel & Tourism**

Most organisations were not explicitly aware of the use of AI in attempted cyber-attacks. However, they assumed that AI was being used in attacks, such as phishing emails. This was generally a concern among organisations, who were particularly worried about highly sophisticated phishing attempts potentially bypassing security systems. For example, there may be fewer grammatical errors in a phishing email, which was a concern for cyber staff because they may not be as easily identified by staff as suspicious.

3.12 Personal data protection and organisational data governance

A new question added in 2025/2026 asked about the protection of personal data. Around one in seven businesses (14%) and one in five charities (22%) said they held personal data that was not protected by techniques such as anonymisation or encryption, suggesting that the majority do protect personal data (77% of businesses and 69% of charities). Businesses in administration or real estate (19%) and agriculture, forestry or fishing (25%) were significantly more likely to report holding personal data that was not protected by anonymisation or encryption.

Around half of businesses (51%) and charities (47%) said they had specific rules for storing and moving personal data files. Of those reporting that they did anonymise and encrypt personal data, only around half of businesses (52%) and charities (49%) reported having specific rules for storing and moving personal data files.

When organisations were asked about data protection in the qualitative interviews, charities and larger businesses seemed more stringent about protections. This was usually associated with protecting personal data

handling and the fear that personal data could be stolen. Organisations seemed aware that stolen personal data could be sold onwards, and this was often assumed to be avoided by the encryption of sensitive or personal data.

However, a few organisations in the qualitative interviews made assumptions about protections, such as encryption, but did not seem certain to know if the data was encrypted or not. This was particularly relevant when an organisation held data in a supplier's system. One large business mentioned that the data is encrypted in-house, but when the client takes ownership of the data they do not have visibility of how it is handled.

> "It depends what flavour of service our clients are taking as to what degree of ownership of that degree of security we have. It's the client's machine in our shed, so we don't have any hands on it whatsoever, apart from cooling it down and providing electricity into it and possibly a network connection. What they run on it is nothing to do with us. It could be unspeakably awful, but it's not our business." **Large business, Information and communications sector**

One charity mentioned the potentially devastating impacts of a breach on customers, as well as the impact of a previous breach.

> "We've been quite conservative for a long time. Firstly, because I know there was a successful phishing attack and then secondly, because the vast majority of our money does come from individual giving. So, we are paranoid about protecting their data because if they don't trust us, we don't exist." **Charity, England and Wales**

Chapter 4: Prevalence and impact of cyber breaches or attacks

This chapter explores the nature, extent and impact of cyber breaches and attacks on organisations over the past year. We also provide broad estimates of the financial cost of these breaches and attacks.

Across these findings, the survey aims to account for all the types of breaches or attacks that organisations might face. This includes accidental breaches, as well as ones perpetrated intentionally. It also includes recorded cyber breaches and attacks that did not necessarily get past an organisation's defences (but attempted to do so). Furthermore, we isolate

and discuss the cases that had a material outcome, such as a loss of money, assets, or data.

It is important to remember the survey only includes the breaches or attacks that organisations were able to identify and willing to report. There are likely to be hidden attacks, and other breaches that go unidentified, so the findings reported here may underestimate the full extent of the prevalence of cyber breaches and attacks.

To note, there is a separate chapter (Chapter 6) that covers similar statistics specifically on prevalence and financial impact of cyber breaches and attacks which meet the definition of cyber crime,[footnote 10] as well as the prevalence of fraud that occurred as a result of a cyber breach or attack. Cyber crimes are a subset of all cyber security breaches and attacks and where cyber crimes are being referred to it is made explicit in the text.

Key takeaways

- Just over four in ten businesses (43%) and around three in ten charities (28%) reported having observed any kind of cyber security breach or attack in the last 12 months.
- Using our results to extrapolate to the wider UK business population, this equates to approximately 612,000 businesses and 57,000 charities having identified a cyber breach or attack in the last 12 months.
- Following the pattern observed in previous years, medium (65%) and large (69%) businesses were more likely to have experienced a cyber breach or attack in the last 12 months compared to micro (42%) and small (46%) businesses.
- Overall prevalence of experiencing any cyber breach or attack has remained in line with last year, after a significant decline the previous year (from 50% in 2023/2024 to 43% in 2024/2025).
- Phishing attacks remained the most prevalent type of breach or attack by far (experienced by 38% of businesses and 25% of charities) and continued to be ascribed as the most disruptive type of breach or attack (69% of businesses and 69% of charities that experienced a breach or attack). Whilst the prevalence of phishing attacks among all organisations did not increase, among those who experienced a breach or attack, the proportion experiencing phishing attacks only has increased among both businesses (from 45% last year to 51% this year) and charities (from 46% last year to 57% this year). The qualitative interviews highlighted a perception that phishing attacks had become easier for attackers to commit and this was contributing to a perceived increase in the volume of attacks.

- Ransomware attacks among businesses have declined compared with the previous two years (1% this year down from 3% in both 2024/2025 and 2023/2024) and phishing attacks and impersonation breaches or attacks, whilst not significantly different to last year, have significantly declined compared to two years ago (38% this year down from 42% in 2023/2024). Impersonation breaches or attacks have decreased to 12% this year, down from 17% in 2023.
- Among charities there have been significant decreases in the proportion of charities experiencing impersonation breaches or attacks and experiencing a takeover. Impersonation breaches or attacks were significantly down compared with the previous two years (7% this year down from 11% in 2024/2025 and 12% in 2023/2024). The proportion of charities experiencing a takeover has decreased from 3% in 2024/2025 to 1% this year (although remains in line with 2% in 2023/2024).
- The proportion of businesses and charities experiencing any negative outcome has remained consistent with 2024/2025 (19% for business and 11% for charities in 2025/2026 compared to 16% for both businesses and charities in 2024/2025). However, there has been an increase in businesses reporting that the breach or attack led to loss of revenue or share value (2% in 2024/2025 to 5% in 2025/2026) and an increase in those reporting it results in reputational damage (1% in 2024/2025 to 3% in 2025/2026).
- The median perceived cost of the most disruptive breach or attack was £0 for businesses and £0 for charities, increasing to £30 for medium and large businesses. The range of perceived cost where most fell (25th to 75th percentile) was £0 to £200 for businesses and £0 to £80 for charities, suggesting that the majority of businesses did not experience high costs. Looking at the perceived cost for the top 5% of cases (95th percentile), however, does show that in a minority of cases organisations can face high costs (£4,000 for all businesses and micro/small businesses, rising to £10,000 for medium/large businesses, and £1,000 for charities). Perceived costs were higher when an outcome from the breach or attack was experienced or when just those who had a material financial cost (not £0) were included.

4.1 Note on comparability to previous year

In the 2023/2024 survey some significant wording changes were made to the question that sought to capture overall incidence of cyber breaches and attacks (Q53A). This means results for overall incidence of cyber breaches and attacks (Q53A) can only be compared to the 2023/2024 and 2024/2025 waves of the survey and not to any years prior.

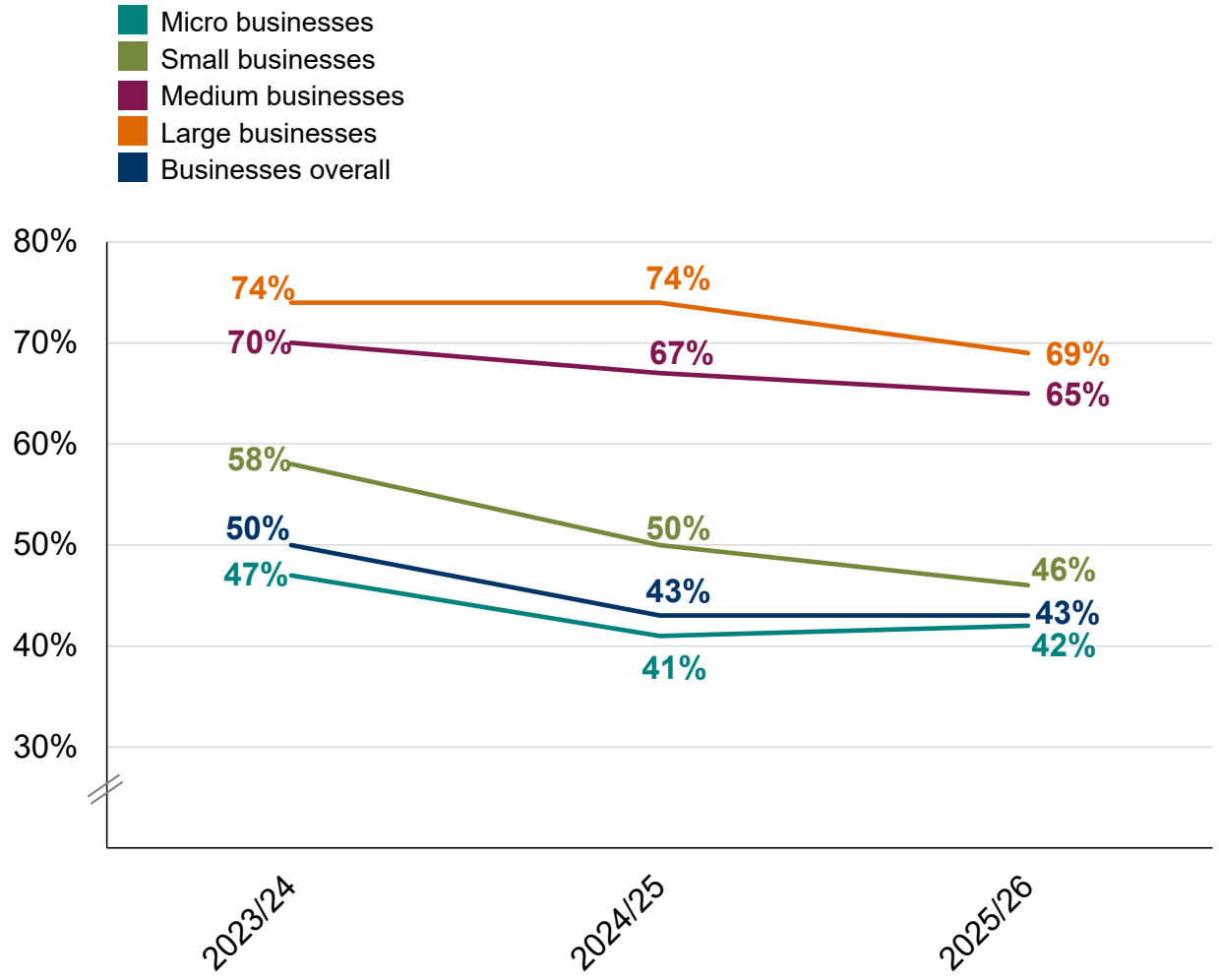
4.2 Identified breaches or attacks

Over four in ten businesses (43%) and around three in ten charities (28%) reported having experienced any kind of cyber security breach or attack in the last 12 months[footnote 11]. This accounts for approximately 612,000 businesses and 57,000 registered charities, although these estimates, like all survey results, are subject to a margin of error (see Appendix A).

As shown in Figure 4.1, medium (65%) and large (69%) businesses were more likely to have experienced a cyber breach or attack in the last 12 months compared to micro (42%) and small (46%) businesses. Lower prevalence in micro and small businesses compared to medium and large businesses was also observed for prevalence of cyber crimes, presented in Chapter 6. These findings may indicate poorer identification and reporting practices in smaller organisations as they may have less sophisticated cyber security monitoring in place.

Trends over time
Prevalence of cyber security breaches or attacks amongst businesses remained exactly in line with last year (43% in 2024/2025 and 2025/2026), as outlined in Figure 4.1. This follows a significant decline in the prevalence of breaches or attacks amongst businesses last year (from 50% in 2023/2024 to 43% in 2024/2025), which was driven by a decrease among small and micro businesses.

Figure 4.1: Percentage of businesses over time that have identified breaches or attacks in the last 12 months



bases 2025/2026: 1,154 micro businesses; 507 small businesses; 296 medium businesses; 155 large businesses; 2,112 businesses overall
bases 2024/2025: 1,013 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,179 businesses overall
bases 2023/2024: 1,060 micro businesses; 506 small businesses; 264 medium businesses; 170 large businesses; 2,000 businesses overall

Looking at prevalence of cyber breaches or attacks by sector (Figure 4.2), businesses in the information and communication sector (63%) and the professional, scientific or technical sector (54%) were significantly more likely than businesses overall to have identified breaches or attacks in the last 12 months. Businesses less likely to have identified breaches or attacks in the last 12 months include those in the food or hospitality sector (33%) and the retail or wholesale sector (31%).

Figure 4.2 : Percentage of businesses that have identified breaches or attacks in the last 12 months, by sector

Change to table view

Information and communication	63%

Professional, scientific or technical	54%
Utilities or production	49%
Administration or real estate	48%
Construction	45%
Transport or storage	45%
Finance or insurance	44%
Entertainment or service	42%
Agriculture, forestry or fishing	36%
Health or social care	33%
Food or hospitality	33%
Retail or wholesale	31%
Businesses overall	43%

Bases: 81 information and communication businesses; 217 professional, scientific or technical businesses; 205 utilities or production businesses; 306 administration or real estate businesses; 262 construction businesses; 85 transport or storage businesses; 101 finance or insurance businesses; 163 entertainment or service businesses; 69 agriculture, forestry or fishing; 101 health or social care businesses; 184 food or hospitality businesses; 302 retail or wholesale businesses; 2,112 businesses overall

Prevalence of cyber breaches and attacks varied little by region, but businesses in Northern Ireland were less likely than businesses overall to have experienced a breach or attack (33% compared to 43% of all businesses). However, it is worth noting that regional analysis of prevalence will be influenced by other factors, such as the distribution of business sectors.

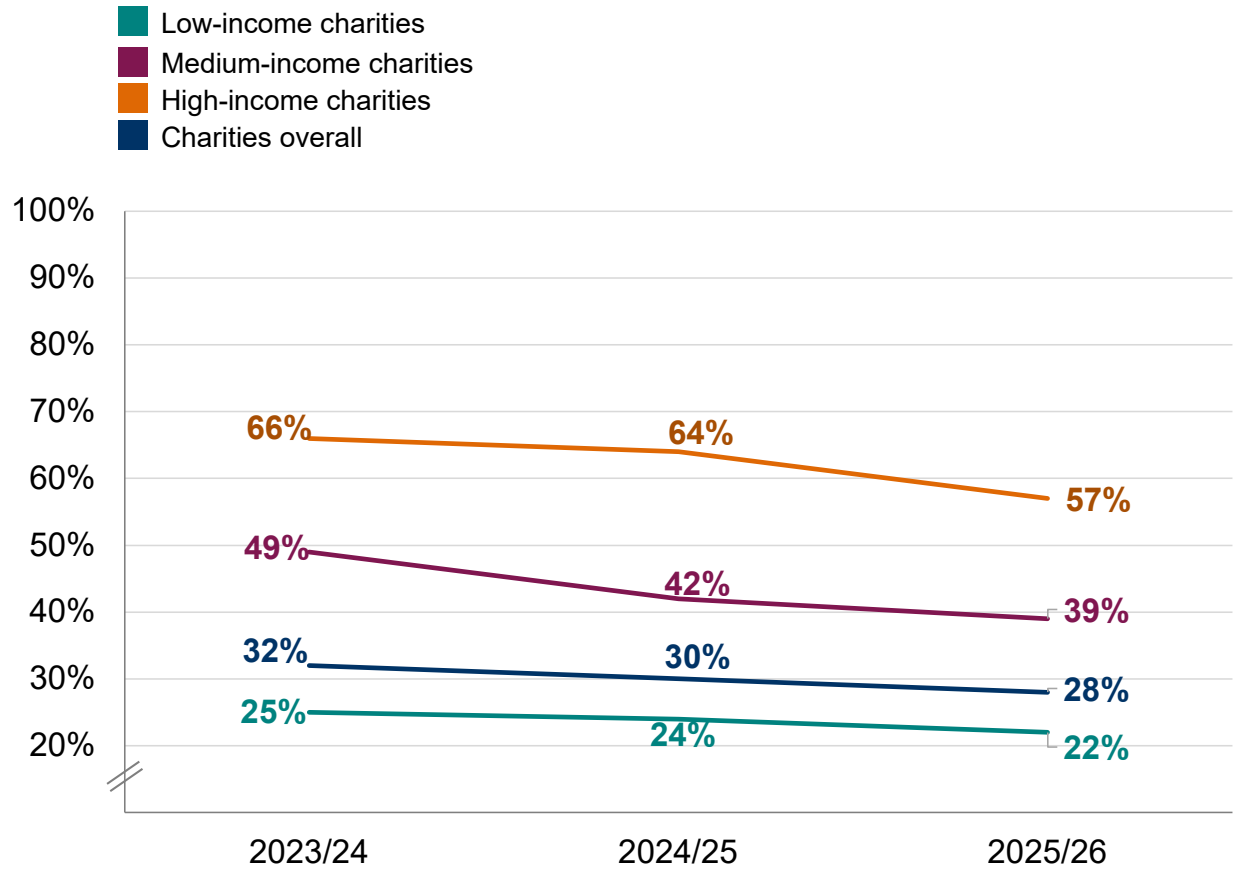
For charities a similar picture to businesses emerges (Figure 4.3), where medium-income charities (39%) and high-income charities (57%) were significantly more likely to have identified a breach or attack compared to low-income charities (22%) and to charities overall (28%).

Trends over time

Prevalence of cyber security breaches or attacks amongst charities (Figure 4.3) has remained in line with last year (28% compared to 30% in 2024/2025) and there has also been no significant change in prevalence of

attacks or breaches by charity size compared to last year. However, compared to 2023/24 there has been a significant decline in cyber breaches or attacks among high-income charities (66% in 2023/24 compared to 57% in 2025/26).

Figure 4.3: Percentage of charities over time that have identified breaches or attacks



Bases: 2025/26: 496 low-income charities, 254 medium-income charities, 335 high-income charities; 1,085 charities overall
Bases: 2024/25: 446 low-income charities, 292 medium-income charities, 343 high-income charities; 1,081 charities overall
Bases: 2023/24: 464 low-income charities, 205 medium-income charities, 335 high-income charities; 1,004 charities overall

Types of breaches or attacks identified, among all organisations
Figure 4.4 shows the types of breaches and attacks that organisations report having. The most common by far was phishing (38% of businesses and 25% of charities) defined in the context of this survey as staff receiving fraudulent emails or being directed to fraudulent websites.

Phishing attacks were followed, to a much lesser extent, by people impersonating organisations in emails or online (12% of businesses and 7% of charities) and then viruses or other malware (7% of businesses and 3% of charities).

Figure 4.4 : Percentage of types of breaches or attacks in the last 12 months, among all organisations

Change to table view

Type	Businesses	Charities
Phishing attacks	38%	25%
People impersonating, in emails or online, organisation or staff	12%	7%
Devices targeted with malware (viruses/spyware)	7%	3%
Hacking or attempted hacking of online bank accounts	3%	1%
Denial of service attacks	3%	1%
Takeovers/attempts to take over website/social media accounts/email	2%	1%
Devices being targeted with ransomware	1%	1%
Unauthorised accessing of files/networks by staff, even if accidental	1%	1%
Unauthorised accessing of files/networks by people outside organisation (other than staff)*	1%	0%
Unauthorised listening into video conferences or instant messaging*	0%	0%
Other types of cyber security breaches or attacks	2%	1%

Bases: 2,112 businesses, 1,085 charities
*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as “less than 0.5%”.

Large businesses, and to a slightly lesser extent, medium businesses, were more likely to report most cyber breaches and attacks compared to businesses overall, including:

- Phishing attacks (63% of large businesses and 60% of medium businesses compared to 38% of businesses overall)
- People impersonating, in emails or online, organisation or staff (47% of large businesses and 38% of medium businesses compared to 12% of businesses overall)
- Devices targeted with malware (viruses/spyware) (23% of large businesses and 12% of medium businesses compared to 7% of businesses overall)
- Denial of service attacks (9% of large businesses and 5% of medium businesses compared to 3% of businesses overall)
- Takeovers/attempts to take over website/social media accounts/email (5% of large businesses and 5% of medium businesses compared to 2% of businesses overall)
- Devices being targeted with ransomware (7% of large businesses and 3% of medium businesses compared to 1% of businesses overall)
- Unauthorised accessing of files/networks by staff, even if accidental (6% of large businesses and 3% of medium businesses compared to 1% of businesses overall)
- Unauthorised accessing of files/networks by people outside organisation (other than staff) (3% of large businesses compared to 1% of businesses overall)
- Unauthorised listening into video conferences or instant messaging* (2% of large businesses compared to less than 0.5% of businesses overall)
- Other types of cyber security breaches or attacks (7% of large businesses and 4% of medium businesses compared to 2% of businesses overall)

The same pattern was true for charities, with high-income charities much more likely to report a range of breaches or attacks compared with charities overall:

- Phishing attacks (50% of high-income charities compared to 25% of charities overall)
- People impersonating, in emails or online, organisation or staff (34% of high-income charities compared to 7% of charities overall)
- Devices targeted with malware (viruses/spyware) (10% of high-income charities compared to 3% of charities overall)
- Denial of service attacks (3% of high-income charities compared to 1% of charities overall)
- Hacking or attempted hacking of online bank accounts (4% of high-income charities compared to 1% of charities overall)

- Devices being targeted with ransomware (4% of high-income charities compared to 1% of charities overall)
- Unauthorised accessing of files/networks by staff, even if accidental (4% of high-income charities compared to 1% of charities overall)
- Unauthorised accessing of files/networks by people outside organisation (1% of high-income charities compared to less than 0.5% of charities overall)
- Other types of cyber security breaches or attacks (2% of high-income charities compared to 1% of charities overall)

Trends over time among all organisations

Ransomware attacks among businesses have declined compared with the previous two years (1% this year down from 3% in both 2024/2025 and 2023/2024). Looking at differences by business size, there was a significant decrease among micro businesses between 2023/2024 (3%) and this year (1%). Phishing attacks and impersonation breaches or attacks, whilst not significantly different to last year, have significantly declined compared to two years ago. Just under four in ten businesses experienced phishing this year (38%), a decrease from just over four in ten (42%) in 2023/2024. This was largely driven by a significant decrease among small businesses (from 49% in 2023/2024 to 40% this year). Impersonation breaches or attacks have decreased to 12% this year, down from 17% in 2023/2024 and significant decreases were observed among all sizes of business.

Among charities there have been significant decreases in the proportion of charities experiencing impersonation breaches or attacks and experiencing a takeover. Impersonation breaches or attacks are significantly down compared with the previous two years (7% this year down from 11% 2024/2025 and 12% in 2023/2024). This decline was driven by decreases among low-income charities (4% this year down from 7% 2024/2025 and 8% in 2023/2024) and medium-income charities (9% this year down from 15% 2024/2025). The proportion of charities experiencing a takeover has decreased from 3% in 2024/2025 to 1% this year (although was in line with 2% in 2023/2024). The decrease was again largely driven by low-income charities (3% of all low-income charities in 2024/2025 compared to 1% of low-income charities this year).

Types of breaches or attacks identified, among organisations identifying a breach or attack in the last 12 months

Figure 4.5 shows the types of breaches and attacks that organisations report having, as a proportion of only those that have identified any in the last 12 months. Following the same pattern as when looking at all organisations, the most common by far was phishing (88% among affected businesses and 87% among affected charities), followed to a much less extent by impersonation (28% of businesses and 26% of charities identifying a breach or attack).

Figure 4.5 : Percentage of types of breaches or attacks in the last 12 months, among organisations that have identified any breaches or attacks

Change to table view

Type	Businesses	Charities
Phishing attacks	88%	87%
People impersonating, in emails or online, organisation or staff	28%	26%
Devices targeted with malware (viruses/spyware)	16%	12%
Hacking or attempted hacking of online bank accounts	8%	4%
Denial of service attacks	6%	4%
Takeovers/attempts to take over website/social media accounts/email	5%	4%
Devices being targeted with ransomware	3%	3%
Unauthorised accessing of files/networks by staff, even if accidental	2%	2%
Unauthorised accessing of files/networks by people outside organisation (other than staff)	2%	1%
Unauthorised listening into video conferences or instant messaging*	0%	2%
Other types of cyber security breaches or attacks	4%	2%

Bases: Those that identified a breach or attack in the last 12 months: 1,026 businesses, 422 charities

*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as “less than 0.5%”.

Trends over time among organisations identifying a breach or attack in the last 12 months

Whilst the prevalence of phishing attacks among all organisations did not increase, among those who experienced a breach or attack in the last 12 months, the proportion experiencing phishing attacks, and no other type of breach or attack, has increased among both businesses (from 45% last year to 51% this year) and charities (from 46% last year to 57% this year).

The other trends mimic those seen among all organisations, with a decrease in businesses experiencing ransomware (3% of all businesses experiencing a breach or attack this year compared to 6% in 2024/25 and 2023/24) and impersonation (28% of all businesses experiencing a breach or attack this year compared to 34% in 2024/25 and 35% in 2023/24).

For charities experiencing a breach or attack there was a decrease in the proportion experiencing takeovers (4% of all charities experiencing a breach or attack this year compared to 9% in 2024/25).

4.3 Frequency of breaches or attacks

Among those identifying any breach or attack in the previous 12 months, as shown in Figure 4.6, around three in ten businesses (29%) and around a quarter of charities (26%) said they experienced a breach or attack at least weekly. Around a fifth experienced a breach or attack once a month (22% of businesses and 18% of charities) and slightly more said they experienced this less than once a month (27% of businesses and 29% of charities).

Figure 4.6 : How often organisations have experienced breaches or attacks in the last 12 months

Change to table view

Organisation type	% Only Once	% Less than once a month	% Once a month	% Weekly or more	% Don't know	Total
Businesses	19	27	22	29	1	
Charities	24	29	18	26	4	

Bases: Those that identified a breach or attack in the last 12 months: 1,026 businesses, 422 charities

Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

Whilst frequencies of breaches or attacks in the last 12 months remained static among businesses, there was a significant increase in the proportion of charities saying they experienced cyber breaches or attacks weekly or more (from 18% in 2024/2025 to 26% in 2025/2026). This was driven largely by an increase among medium-income charities (from 13% in 2024/2025 to 24% in 2025/2026).

4.4 The breaches or attacks considered most disruptive

Among the organisations that reported having had breaches or attacks in the past 12 months, phishing attacks were commonly reported as the most disruptive types of attack (by 69% of the businesses and 69% of the charities). Figure 4.7 also shows that people impersonating organisations or staff was the next most commonly reported breach or attack to be disruptive.

Figure 4.7 : Percentage that report the following types of breaches or attacks as the most disruptive, across all who specified a breach or attack

Change to table view

Type	Businesses	Charities
Phishing attacks, i.e. staff receiving fraudulent emails or arriving at fraudulent websites	69%	69%
People impersonating, in emails or online, your organisation or your staff	13%	16%
Hacking or attempted hacking of online bank accounts	4%	3%
Your organisation’s devices being targeted with other malware (e.g viruses or spyware)	4%	2%
Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services	3%	2%
Takeovers or attempts to take over your website, social media accounts or email accounts	2%	3%

Type	Businesses	Charities
Your organisation’s devices being targeted with ransomware	1%	2%
Unauthorised accessing of files/networks by people outside organisation (other than staff)	1%	1%
Unauthorised accessing of files/networks by staff, even if accidental*	0%	1%
Unauthorised listening into video conferences or instant messaging*	0%	0%
Other types of cyber security breaches or attacks	2%	2%

Bases: Those that were able to specify a breach or attack experienced in the last 12 months: 970 businesses, 388 charities
*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as “less than 0.5%”.

Micro businesses (70%) were significantly more likely than medium (59%) and large (53%) businesses to have identified phishing as the most disruptive breach. Whereas large (31%), medium (26%) and small (18%) businesses were significantly more likely to have stated impersonation as the most disruptive breach compared to micro businesses (11%). Large businesses were also significantly more likely than businesses overall to cite denial of service attacks (6% compared with 3% of businesses overall) and unauthorised accessing of files or networks by people outside of the organisation (3% compared with 1% of businesses overall) as their most disruptive attack.

As well as there being a decrease of impersonation breaches and attacks among organisations this year, there was also a downward trend for citing impersonation as the most disruptive attack. This year 13% of businesses who had experienced breaches or attacks cited impersonation as the most disruptive, significantly lower than 18% in 2024/2025 and 17% in 2023/2024. Likewise, charities were less likely to cite impersonation (16%) compared to 24% in 2023/2024.

Diagnosing why phishing attacks were the most disruptive breach or attack

Those that experienced more than one type of breach or attack and then selected phishing as the most disruptive type of attack, or who only experienced phishing, were asked a follow up question about why the phishing attack was the most disruptive. The most common reason given

was staff time spent on investigating potential attacks (21% businesses and 16% charities). This was followed by time needed for staff training (12% businesses and 8% charities) and downtime for the organisation, such as staff not being able to work while investigations were ongoing (12% businesses and 4% charities). A minority said it was because they had to invest in new systems to protect against future attacks (5% business and 3% charities).

It is worth noting that two-thirds of businesses (66%) and around three-quarters of charities (76%) responded 'none of these' when prompted with a range of reasons for phishing attacks being disruptive. This suggested it was possible there were a range of other reasons for phishing attacks being disruptive that have not currently been captured by the survey.

As in 2024/2025, organisations in the qualitative interviews felt that the sheer volume of phishing attacks received led to staff time in dealing with each of these, even if it was just investigating it and then doing nothing further. For some organisations it was a daily occurrence that could not be ignored. Large businesses, especially, typically experienced huge volumes of daily phishing attacks.

> "We've seen a noticeable increase in phishing attempts, of emails pretending to be senior staff." **Large business, Health/social care**

> "Over 1,000 phishing attempts are blocked weekly." **Large business, Administration/real estate**

There was a sense that phishing had become easier and more accessible for attackers which was contributing to a perceived increase in the volume of attacks. For instance, one large travel and tourism business felt that there was a noticeable increase in amateur hackers using 'kiddie' scripts that are freely available on the internet, attempting phishing attacks:

> "We're seeing quite a big increase in the number of amateurs, who can access what we call kiddie scripts, that are attempting to access the network, from a simple port probe to the routers, to more sophisticated techniques to try and gain access." **Large business, travel and tourism**

One large business detailed a more complex form of phishing, vishing, which is the use of fraudulent phone calls or voice messages rather than emails. The attempted breach was concerning since it involved long lead times conducted by cyber criminals:

> “We suffered what’s now known as a vishing attack that was cleverly constructed…they nearly got away with half a million pounds. They didn’t realise that the hackers had conducted 12 months prior background research on that person.” **Large business, Travel & Tourism**

It was unclear whether the perceived increase in phishing attacks, particularly among larger organisations, was due to an actual increase in targeted attacks, or due to the growing sophistication of IT resources and software that were able to monitor phishing attacks.

Strategies varied widely to monitor and prevent or block phishing attacks, demonstrating the diverse ways businesses and charities managed their cyber threats. For instance, larger organisations tended to focus on continuous training of staff, noting that staff were a common point of weakness in their cyber security defences. Smaller organisations tended to mention initial training when staff joined, but a lack of resource prevented continuous training. It was noted across the board that it was a challenge to get staff buy-in, that is, staff believing that IT issues and cyber security were important.

> “When I first started three years ago, staff used to all log in with just one account. And those passwords barely got changed unless somebody forgot it. [Healthcare staff] are there to care, not to, you know, think about IT issues.” **Charity, England**

The role of staff training on cyber security was therefore viewed as crucial and some organisations said that they had been leveraging the recent high-profile cyber-attacks as a way to highlight to staff the importance of good cyber security practices. Some organisations, particularly smaller businesses and charities, felt they were constrained in the amount of staff training they could do due to budgets and expressed their desire for cheaper or free training and education tools to improve their cyber security posture.

> “The biggest problem that I think faces IT professionals is getting across to people the education side of it. Ultimately cyber security is the responsibility of end users, so it’s very much an education thing.” **Medium business, Transport or storage**

> “I wish there was more interacting or more guidance or more courses that were out there. You can either pay a fortune, but when you’re a

> charity, it’s not the best. It would be nice to have some free tools.”
> **Charity, England**

General improvement of software or IT processes was also another common strategy for dealing with phishing attempts.

Whilst organisations typically had software in place for monitoring phishing attacks, they rarely used this software to proactively track or analyse the results. For example, one small business in the information and communication sector reported no “systematic” monitoring of attempted cyber breaches, despite a high level of awareness of risk of the attacks. Similarly, a charity in the healthcare sector described being made aware of increased phishing attacks due to staff reporting high levels to IT, rather than IT tracking these levels independent of staff reports.

Time taken to recover from the most disruptive breach or attack
When considering their most disruptive breach or attack, the vast majority of businesses (87%) and charities (91%) affected reported being able to restore their operations within 24 hours (Figure 4.8). Furthermore, more than seven in ten businesses (72%) and charities (76%) said it took ‘no time at all’ to recover.

Figure 4.8 : How long it took to get operations back to normal after their most disruptive breach or attack was identified

Change to table view

Organisation type	% No time at all	% Less than a day	% More than a day	% Don’t know	Total
Businesses	72	15	12	1	
Charities	76	15	7	1	

Bases: Those that were able to specify a breach or attack experienced in the last 12 months: 970 businesses, 388 charities
Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

Among businesses, the time taken to get operations back to normal after their most disruptive breach has increased. Fewer now say that it took them less than a day (87% compared with 92% in both 2024/2025 and 2023/2024). This looks to be driven by the smallest businesses with a significant decrease in the proportion of micro businesses saying it took

them less than a day (86% compared with 92% in both 2024/2025 and 2023/2024).

4.5 How organisations are affected

Outcomes of breaches or attacks
Among the businesses and charities that experienced any breaches or attacks, around two in ten businesses (19%) and around one in ten charities (11%) also experienced a negative outcome as a result (listed in Figure 4.9). The low proportion stating a negative outcome indicates that a large proportion of attacks are unsuccessful. Temporary loss of access to files or networks (8% businesses and 3% charities) and disruption to websites (6% businesses and 4% charities) were the most commonly reported negative outcomes. However, as Figure 4.8 indicates, cyber breaches and attacks that overcome defences can have a wide range of negative outcomes.

Figure 4.9 : Percentage that had any of the following outcomes, among the organisations that have identified breaches or attacks in the last 12 months

Change to table view

Type	Businesses	Charities
Any listed outcome	19%	11%
Temporary loss of access to files or networks	8%	3%
Your web applications / online services were taken down or made slower	6%	4%
Lost access to any third-party services you rely on	5%	3%
Money was stolen	3%	2%
Compromised accounts or systems used for illicit purposes	3%	2%
Software or systems were corrupted or damaged	3%	1%
Organisational data was altered, destroyed or taken	2%	1%

Type	Businesses	Charities
Physical devices or equipment were damaged or corrupted	2%	1%
Money was paid as a ransom	2%	1%
Personal data was altered destroyed or taken*	2%	0%
Permanent loss of files (other than personal data)	1%	1%
Lost or stole assets, trade secrets or intellectual property*	0%	1%

Bases: Those that identified a breach or attack in the last 12 months: 1,026 businesses, 422 charities

*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as “less than 0.5%”.

Whilst in 2024/2025 large and medium businesses were more likely than businesses overall to have experienced any listed outcome in Figure 4.8, this year there was no difference by business size. However, the one measure large businesses were more likely to experience was lost or stolen assets, trade secrets or intellectual property (3% compared to less than 0.5% of businesses overall).

Trends over time

The proportion of businesses and charities experiencing a negative outcome has remained relatively consistent with 2024/2025 (19% for business and 11% for charities in 2025/2026 compared to 16% for both businesses and charities in 2024/2025).

Nature of the impact

Breaches that did not result in negative financial consequences or data loss can still have an impact on organisations. Therefore, other potential impacts were captured and shown in Figure 4.10. Three in ten businesses (30%) and almost three in ten charities (26%) that experienced a breach or attack reported being impacted in at least one of the ways noted in Figure 4.10.

Most commonly, breaches or attacks led to organisations having to take up new measures to prevent or protect against future cases (19% businesses and 15% charities) or having to employ additional staff time to deal with the breach or attack (16% businesses and 17% charities).

Figure 4.10 : Percentage that were impacted in any of the following ways, among the organisations that have identified breaches or

attacks in the last 12 months

Change to table view

Type	Businesses	Charities
Any Listed Impact	30%	26%
New measures needed to protect against future breaches or attacks	19%	15%
Additional staff time to deal with breach or attack or to inform customers or stakeholders	16%	17%
Stopped staff from carrying out their day-to-day work	11%	7%
Any other repair or recovery costs	6%	3%
Loss of revenue or share value*	5%	0%
Complaints from customers	4%	2%
Prevented provision of goods or services to customers	4%	1%
Reputational damage	3%	1%
Discouraged you from carrying out a future business activity	2%	2%
Goodwill compensation or discounts given to customers	1%	0%
Fines from regulators or authorities or associated legal costs*	1%	0%

Bases: Those that identified a breach or attack in the last 12 months: 1,026 businesses, 422 charities

*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as “less than 0.5%”.

The impact was most substantial for large businesses. For example:

- 35% of large businesses said they had to take up new measures to prevent or protect against future breaches or attacks (compared with 19%

all businesses identifying breaches or attacks)

- 30% needed additional staff time to deal with breaches or attacks (compared with 16% of all businesses)

A similar trend was observed for high-income charities. Whereas 26% of all charities identifying breaches or attacks reported an impact, this rose to 42% of high-income charities. In terms of individual impacts for high-income charities:

- 26% needed additional staff time to deal with breaches or attacks (compared to 17% of all charities identifying breaches or attacks)
- 24% said they had to take up new measures to prevent or protect against future breaches or attacks (compared with 15% of all charities identifying breaches or attacks)

Trends over time
New measures being needed and additional staff time remained the two most common impacts, as was seen in 2023/2024 and 2024/2025, and the proportion of businesses (30% in 2025/2026 and 28% in 2024/2025) and charities (26% in 2025/2026 and 30% in 2024/2025) experiencing any of the impacts in Figure 4.9 remained consistent.

However, looking at individual impacts, there has been an increase in businesses reporting that the breach or attack led to loss of revenue or share value (2% in 2024/2025 to 5% in 2025/2026) and an increase in those reporting it results in reputational damage (1% in 2024/2025 to 3% in 2025/2026).

4.6 Financial cost of breaches or attacks

Each year, this survey series has attempted to capture the perceived cost of cyber security breaches or attacks on organisations[footnote 12].

This year, we have stopped reporting the mean costs. Given the distribution of cyber impacts is highly skewed and subject to high sampling error this is not a robust statistical indicator. It can also create a disclosure risk where a dominant share of the total cost is from a limited number of organisations.

The median perceived cost is presented, as well as adding the 25th-75th percentile range where most cases fall, the top 10% of cases (90th percentile) and the top 5% of cases (95th percentile).

There has been a small change in the statistical methodology[footnote 13] used to calculate the median.

As in previous years of the survey, we asked separate questions breaking down different aspects of the cost of the single most disruptive breach or attack that organisations recalled facing in the preceding 12 month period (short-term and long-term direct costs, staff time and other indirect costs). The breakdown for these separate cost questions is provided in the data tables accompanying this publication (see Tables 43 to Table 47).

Tables 4.1a and 4.1b brings together these granular breakdowns for an overall cost estimate for the most disruptive breach or attack. These are presented for all organisations experiencing breaches or attacks (shown in Table 4.1a), as well as those with an actual outcome (shown in Table 4.1b), such as a loss of assets or data. The latter subgroup of organisations tended to face higher costs, as these tables show.

In these tables, in order to create a larger sample size for more robust estimates, we have combined micro and small businesses, and medium and large businesses.

Table 4.1a: Distribution of perceived total cost of the most disruptive breach or attack from the last 12 months

Across organisations identifying any breaches or attacks

	All businesses	Micro/small businesses	Medium/large businesses	All charities
Median perceived cost (midpoint or typical)	£0	£0	£30	£0
Range of perceived cost where most fall (25th to 75th percentile)	£0 to £200	£0 to £190	£0 to £500	£0 to £80
Perceived cost for the top 10% of cases (90th percentile)	£1,500	£1,140	£2,330	£550
Perceived cost for the top 5% of cases (95th percentile)	£4,000	£4,000	£10,000	£1,000

	All businesses	Micro/small businesses	Medium/large businesses	All charities
Base	952	680	272	386

Table 4.1b: Distribution of perceived total cost of the most disruptive breach or attack from the last 12 months, among those identifying a breach or attack with an outcome

Only across organisations identifying a breach or attack with an outcome

	All businesses	Micro/small businesses	Medium/large businesses	All charities
Median perceived cost (midpoint or typical)	£560	£560	£570	£150
Range of perceived cost where most fall (25th to 75th percentile)	£60 to £3,000	£60 to £3,000	£0 to £3,000	£30 to £550
Perceived cost for the top 10% of cases (90th percentile)	£10,000	£10,000	£83,600	£2,000
Perceived cost for the top 5% of cases (95th percentile)	£15,000	£14,440	Effective base size under 50[footnote 14]	Effective base size under 50
Base	169	122	47	59

Table 4.1a shows that the median perceived cost of the most disruptive breach or attack was £0 for businesses and £0 for charities. This only slightly increased when looking at just medium and large businesses, where the median perceived cost was £30. The range of perceived cost where most fell (25th to 75th percentile) was £0 to £200 for businesses and £0 to

£80 for charities, suggesting that the majority of businesses did not experience high costs for their most disruptive breach or attack. Looking at the perceived cost for the top 5% of cases (95th percentile), however, does show that in a minority of cases businesses can face high costs (£4,000 for all businesses and micro/small businesses, rising to £10,000 for medium/large businesses). A median cost of £0 reflects that many organisations reported having no experience of direct financial loss, not that harms are negligible. A small number of incidents result in very large costs, and potential repeat victimisation means financial impacts may be concentrated among a minority.

Table 4.1b shows the perceived cost of the most disruptive breach or attack among those that experienced some form of outcome from the breach or attack. Where outcomes were experienced, costs were higher. For example, among businesses experiencing an outcome, the perceived cost for the top 5% of cases (95th percentile) was £15,000, compared to £4,000 for businesses regardless of whether there was an outcome or not.

Tables 4.2a and 4.2b show the same perceived cost estimate of the most disruptive breach or attacks as in Table 4.1 but exclude any organisation who gave a cost of £0. This is to give a sense of what the financial burden was among those who did have a material financial cost.

As would be expected, the average costs were higher among this group.

Table 4.2a: Distribution of perceived total cost of the most disruptive breach or attack from the last 12 months, excluding those giving a '£0' cost

Across organisations identifying any breaches or attacks

	All businesses	Micro/small businesses	Medium/large businesses	All charities
Median perceived cost (midpoint or typical)	£200	£200	£300	£150
Range of perceived cost where most fall (25th to 75th percentile)	£50 to £1,000	£50 to £1,000	£100 to £1,620	£30 to £500
Perceived cost for the top	£4,800	£4,150	£7,300	£2,000

	All businesses	Micro/small businesses	Medium/large businesses	All charities
10% of cases (90th percentile)				
Perceived cost for the top 5% of cases (95th percentile)	£10,000	£8,300	£28,200	£3,100
Base	474	310	164	202

Table 4.2b: Distribution of perceived total cost of the most disruptive breach or attack from the last 12 months, excluding those giving a '£0' cost, among those identifying a breach or attack with an outcome

Only across organisations identifying a breach or attack with an outcome

	All businesses	Micro/small businesses
Median perceived cost (midpoint or typical)	£940	£800
Range of perceived cost where most fall (25th to 75th percentile)	£200 to £3,500	£200 to £3,500
Perceived cost for the top 10% of cases (90th percentile)	£12,500	£12,500
Perceived cost for the top 5% of cases (95th percentile)	£20,000	£15,000
Base	137	101

Table 4.2a shows that when looking at the perceived cost of the most disruptive breach or attack, excluding those who gave a £0 cost, the median perceived cost rises to £200 among all businesses and micro/small businesses, to £300 among medium/large businesses and to £150 among charities. Whilst the range where most perceived costs fell (25th to 75th percentile) remains relatively low among businesses and charities, looking at the top 5% of cases (95th percentile), shows that some organisations, particularly medium or large businesses (£28,200), can experience very high costs.

Table 4.2b shows the perceived cost of the most disruptive breach or attack among those that experienced some form of outcome, but excluding those giving a cost of £0. Results for medium and large businesses and charities can not be shown in the table due to the effective base size being too low to report on. The table again shows that where outcomes were experienced, costs were higher. For example, among businesses experiencing an outcome, the perceived cost for the top 5% (95th percentile) doubled to £20,000, compared to £10,000 for businesses regardless of whether there was an outcome or not.

Qualitative insights on costs of cyber breaches

Across most organisations, monitoring cyber costs tended to not be a priority. When organisations did measure the financial impact of cyber breaches or attempted cyber breaches, it typically involved monitoring staff time to deal with the incident or the cost of having cyber insurance, rather than anything more detailed.

However, the lack of cyber cost scrutiny was not universal. One charity described a thorough process of calculating how much cyber incidents cost, because they had to justify all the staff time spent away from charitable activities. These costs were helpful in justifying any spend on cyber security in the future as well. Another charity mentioned the scrutiny they received after a breach, but often there were not enough funds proactively received to prevent the attack.

> "Whenever things do go awry or there is a breach people tend to ask an awful lot of questions and one of the biggest ones will always come back [as] 'well we would have liked to have been able to do that, but we didn't have the resource to do it. We weren't given the funding for it at the time.'" **Charity, England**

To secure budgets, some organisations used widespread reports of attacks as leverage to secure funding. One large business in the information and communication sector highlighted the economic environment as detracting from important cyber budget and resource discussions. However, the respondent believed that shifting a narrative out of cyber defence and towards a business staying afloat with examples, helped budget conversations with senior leadership.

> "It's a shifting narrative from cyber defence to the cost of being out of business, which would be horrific. Providing senior leadership a long list of risks helps getting traction." **Large business, information and communication sector**

Chapter 5: Dealing with cyber breaches or attacks

This chapter explores how well businesses and charities deal with breaches or attacks, including identification, response, reporting and adaptation to prevent future cases.

In the survey, questions on this topic were generally framed in terms of the most disruptive breach or attack an organisation had faced in the last 12 months. Most of this chapter is therefore only based on the 43% of businesses and 28% of charities that have identified breaches or attacks, rather than the full sample. Consequently, the size and sector subgroups tended to have very small sample sizes, and subgroup analysis is featured much less in this chapter.

The questions on incident response and ransomware in the first sections were, however, asked of the full sample.

Key takeaways

- The most common responses following a cyber breach or attack continued to centre on internal reporting, including informing directors (81% of businesses and 84% of charities) and keeping an internal record of the incident (62% of businesses and 73% of charities).
- External reporting remained uncommon. Among organisations identifying breaches or attacks, four in ten businesses (40%) and around a third of charities (36%) reported their most disruptive breach outside their organisation.
- Larger organisations were more likely to have formal incident response arrangements in place, including a written incident response plan (57% of medium businesses and 76% of large businesses, compared with 21% of micro businesses). By sector (excluding education), businesses in finance or insurance (53%) and information and communication (49%) were most likely to have a formal incident response plan, compared with 25% of businesses overall.
- Compared with 2024/2025, there were no meaningful year-on-year changes in the overall prevalence of the incident response measures covered in this chapter for businesses or charities. The increases previously seen among small businesses were not repeated in 2025/2026, with small business levels broadly stable (for example, written

guidance on who to notify: 50%; external communications plans: 24%; guidance on external reporting: 44%).

- Following a breach or attack, 61% of businesses and 57% of charities reported taking some form of action to prevent future incidents. The most common was people or training changes (31% of businesses and 37% of charities), and the likelihood of taking action increased with organisation size.

5.1 Incident response

Figure 5.1 shows the actions organisations said they had taken, or would take, in response to a cyber incident, using a prompted list. Continuing trends from previous surveys, by far the top response was to inform senior management, chosen by 81% of businesses and 84% of charities. It was far less common for organisations to say they would inform regulators (49% of businesses, 61% of charities). This was perhaps expected, given that not all sectors are regulated to the same extent. Around five in ten said they take, or would take, each of the other listed actions, except for using an NCSC-approved incident response company, which was cited less frequently (16% of businesses and 13% of charities).

Of those that had cyber insurance, more than half of businesses (52%) and charities (62%) said they would inform their cyber insurance provider in the event of a cyber security breach or attack.

Figure 5.1 : Percentage of organisations that say they take, or would take, the following actions following a cyber security breach or attack

Change to table view

Action	Businesses	Charities
Inform your directors/trustees/governors of the incident	81%	84%
Keep an internal record of incidents	62%	73%
Assess the scale and impact of the incident	59%	69%
Formal debriefs or discussions to log any lessons learnt	57%	65%

Action	Businesses	Charities
Inform your cyber insurance provider (among those who have cyber insurance)*	51%	62%
Attempt to identify the source of the incident	50%	49%
Inform a regulator of the incident when required	49%	61%
Inform your immediate suppliers and/or wider supply chain	47%	38%
Use an NCSC-approved incident response company	16%	13%

Bases: 2,112 businesses; 1,085 charities

*Asked only of those who have cyber insurance, 496 businesses, 188 charities

Figure 5.2 shows the documentation, guidance and processes that organisations have in place for dealing with cyber security incidents. While organisations often said they would take multiple actions following a breach or attack (see Figure 5.1), a smaller proportion already had supporting measures in place. In 2025/2026, the most common measures were roles or responsibilities assigned to specific individuals (39% of businesses and 31% of charities), written guidance on who to notify (34% of businesses and 28% of charities), and guidance around when to report incidents externally (e.g. to regulators or insurers; 32% of businesses and 30% of charities). Incident response plans were less widespread, with 25% of businesses and 19% of charities having a formal incident response plan in place. It was also notable that 45% of businesses and 54% of charities said they had none of these measures in place.

Figure 5.2 : Percentage of organisations that have the following measures in place for dealing with cyber security breaches or attacks

Change to table view

Measures in place for dealing with cyber security incidents	Businesses	Charities
Roles or responsibilities assigned to specific individuals during or after an incident	39%	31%
Written guidance on who to notify	34%	28%

Measures in place for dealing with cyber security incidents	Businesses	Charities
Guidance around when to report incidents externally (e.g. to regulators or insurers)	32%	30%
A formal incident response plan	25%	19%
External communications and public engagement plans	16%	14%

Bases: 2,112 businesses; 1,085 charities.

As in previous years, larger organisations were more likely than average to say they already had these measures in place. For example, 57% of medium-sized businesses and 76% of large businesses had a formal incident response plan, compared with 21% of micro businesses. Among charities, 49% of high-income charities (£500,000+ income) had a formal incident response plan, compared with 19% of charities overall.

By sector, the most formalised approaches continued to be concentrated in a small number of sectors (excluding education). Businesses in finance or insurance (53%) and information and communication (49%) were most likely to have a formal incident response plan in place, compared with 25% of businesses overall.

Trends over time

Compared with 2024/2025, there were no meaningful year-on-year changes in the overall prevalence of the measures shown in Figure 5.2 for businesses or charities. For example, the proportion with a formal incident response plan remained broadly similar (23% of businesses in 2024/2025 vs 25% in 2025/2026; 22% of charities vs 19%), and the same was true for written guidance on who to notify (34% of businesses in both years; 31% of charities vs 28%). The increases among small businesses noted in the previous wave were not repeated in 2025/2026, with small business levels broadly stable (e.g. written guidance on who to notify: 55% in 2024/2025 vs 50% in 2025/2026; external communications plans: 29% vs 24%; guidance on external reporting: 48% vs 44%).

Ransomware payments

Around half of businesses (49%) and a third of charities (34%) had a rule or policy to not pay ransomware demands, which was consistent with 2024/2025 (businesses 52% and charities 38%). However, there was still a high level of uncertainty among organisations on this topic, with one in four businesses (24%) and one in five charities (21%) saying they did not know what their organisation’s policy on this was.

Qualitative insights on incident response plans

Whilst most organisations had some form of incident response plan, these varied in sophistication and continued to be largely untested or incomplete. Only a minority of organisations reported comprehensive testing of incident response plans. This false sense of preparedness, by possessing an incident response plan that lacks testing, could lead to organisational risk. Some organisations highlighted they were aware and concerned about this risk.

Organisations tended to reference plans in a ‘staff handbook’ or ‘continuity plan’ that they were not aware had ever been tested, or at least not tested recently. Some plans were only tested due to post-incident reviews which were mandated by their industry.

> “[Our incidence response plan is] not fully documented and has not been tested. This keeps me awake at night.” **Large business, Manufacturing**

> “The incident response plan is in the staff handbook but we haven’t tested it at all.” **Small business, Administration/real estate**

One smaller charity mentioned they did not have a plan at all, and would not know what to do in the event of an attack.

> “I don’t know, we would probably play it by ear.” **Charity, England and Wales**

However not all organisations left their incident response plans untested. One large organisation in the entertainment sector discussed how they implemented a table-top exercise to test the incident response plan. The exercise involved imagined scenarios that staff had to think about how the business would respond to that, and the different options that could have arisen from the imagined scenario. The exercise resulted in good questions from the IT department. As a result, the business also planned to conduct the same table-top exercise in the wider organisation.

> “I donned my wizard hat… sort of like a Dungeons and Dragons thing where I was the master and I set up the scenario. We designed one around a cyber ransomware attack. We had a bit of fun and it did raise a few good questions.” **Large business, Entertainment/membership**

This example shows that creativity around plan testing could reduce barriers to completion, while achieving productive results.

5.2 External reporting of breaches or attacks

External reporting of breaches was not widespread among organisations. In 2025/2026, even after excluding cases where organisations only reported their most disruptive breach to an outsourced cyber security or IT provider, relatively few organisations reported externally to any single destination (Figure 5.3).

Figure 5.3 highlights that, among businesses who reported externally (beyond "provider-only" cases), the most common places they reported to were banks/building societies/credit card companies (26%), followed by internet or network service providers (11%) and Action Fraud[footnote 15] (9%). Reporting to suppliers/business partners (8%), the police (6%), and other government agencies (10%) was less common.

For charities, the main external reporting destinations were different: the Information Commissioner's Office (ICO) (16%) was the most commonly mentioned destination, followed by internet or network service providers (14%), banks/building societies/credit card companies (13%), and Action Fraud (12%). Charities were also more likely than businesses to report to the police (9%) in this rebased group.

Figure 5.3 : Percentage of organisations reporting their most disruptive breach or attack in the last 12 months to the following groups, among those that reported externally (beyond cyber security or IT providers)

Change to table view

Reporting destination	Businesses	Charities
Bank, building society or credit card company	26%	13%
Internet/Network Service Provider	11%	14%
Other government agency	10%	11%
Action Fraud	9%	12%
Suppliers/business partners	8%	7%

Reporting destination	Businesses	Charities
report@phishing.gov.uk	7%	10%
Police	6%	9%
Company/source of breach	6%	5%
Outsourced cyber security provider	6%	1%
Clients/customers	5%	3%
Social media site (e.g. Facebook)	3%	0%
Website administrator	3%	1%
Information Commissioner's Office (ICO)	2%	16%
Antivirus company	2%	0%
National Crime Agency (NCA)	2%	0%
Cyber Security Information Sharing Partnership (CISP)	1%	1%
Professional/trade/industry association*	1%	0%
National Cyber Security Centre (NCSC)*	0%	1%
Other	4%	11%

Bases: Those that reported their most disruptive breach externally (to someone other than an outsourced cyber security or IT provider, or a parent company): 204 businesses; 91 charities
*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as "less than 0.5%".

In terms of changes over time as to where businesses reported breaches externally, there was a decrease in those reporting to the National Cyber Security Centre (NCSC) (5% in 2023/24 and 4% in 2024/25, dropping to less than 0.5% this year). For charities there was an increase in the proportion reporting a breach to the Information Commissioner's Office (ICO) this year (16%), up from 3% in 2023/24 and 5% in 2024/25. For the first time report@phishing.gov.uk also emerged as somewhere that breaches were being reported, by 7% of businesses and 10% of charities.

Among the businesses and charities that did not report their most disruptive breach or attack, the most common reason given for this was that it was not

considered significant enough to warrant reporting (for 72% of businesses and 73% of charities this was the case). Beyond this, the next most common reasons were:

- they did not know who to report to (10% of businesses and 7% of charities)
- they did not think reporting would make any difference (5% businesses and 3% charities)
- they dealt with the breach internally (3% businesses and 7% charities)

Qualitative insights on organisation's attitudes to reporting and data protection

Organisations tended to view the Information Commissioner's Office as a positive body to report incidents to, while respondents held mixed reviews about the usefulness of Action Fraud[footnote 16]. Most organisations stated they would report serious incidents when they deemed necessary. However, there were often informal definitions being used as to what would constitute an incident as necessary to report. Personal data breaches or large financial loss seemed to be the main drivers of reporting an incident.

Charities were likely to know the processes of reporting any cyber incidents, however this was not universal. One smaller charity mentioned they did not know they had to report an incident, after they paid a fraudulent invoice. They did not have a formal cyber strategy at all, nor encryption for their data, and recognised they were "behind the curve" on their cyber security approach.

> "I guess I didn't report it because I didn't know I had to report it." **Charity, England**

When organisations were asked about data protection, charities and larger businesses seemed more stringent about protections. A few organisations made assumptions about protections, such as encryption, but did not seem certain to know if the data was encrypted or not.

> "We tend to hold all our customers data on an Enterprise Resource System (ERP) that we have in house and really that data on that system is not encrypted in any way. So, it is just about protecting who has access to it in terms of users. So basically, I suppose the answer is if someone got through our firewalls and our edge network and they knew where to look, then, yes, I suppose you could argue we could be a little bit exposed." **Medium business, Wholesale/retail**

One charity mentioned the potentially devastating impacts of a breach on customers, as well as the impact of a previous breach.

> “We’ve been quite conservative for a long time. Firstly, because I know there was a successful phishing attack, and then secondly, because the vast majority of our money does come from individual giving. So, we are paranoid about protecting their data because if they don’t trust us, we don’t exist.” **Charity, England and Wales**

5.3 Actions taken to prevent future breaches or attacks

Among those that identified any breaches or attacks, 61% of businesses and 57% of charities reported taking some form of action to prevent further breaches. As Figure 5.4 shows, the most common action taken was people or training changes (31% businesses, 37% charities).

Likelihood to take some form of action to prevent future breaches and attacks increased with organisation size. Small (69%), medium (74%) and large (84%) businesses were all more likely than micro businesses (58%) to have taken some form of action. Likewise, high-income charities (77%) were more likely to have taken some kind of action compared to charities overall (57%).

Figure 5.4 : Percentage of organisations that have done any of the following since their most disruptive breach or attack of the last 12 months

Change to table view

Action taken since the breach or attack	Businesses	Charities
People or training changes (such as staff training or communications)	31%	37%
Technical changes (such as updated antivirus software)	29%	23%
Governance changes (such as increased monitoring)	8%	7%
Any action taken	61%	57%
No action taken	37%	41%

Bases: All businesses and charities that have only one type of breach experienced, or if they can consider a particular breach or attack: 970 businesses; 388 charities

As may be expected, the picture changed slightly when looking only at businesses and charities whose most disruptive breach or attack resulted in a material outcome (for example the loss of files, money, or other assets). Figure 5.5 shows that the proportion who took some form of action rose to around eight in ten businesses (83%) and close to nine in ten charities (89%). Among those with an outcome, technical changes (such as updated antivirus software or changes to firewall/system configurations) were the most common type of response among businesses (41%), while people or training changes were more common among charities (45%). However, a minority still reported taking no action following an incident with an outcome (14% of businesses and 11% of charities).

Figure 5.5 : Percentage of organisations that have done any of the following since their most disruptive breach or attack of the last 12 months, in cases where breaches had material outcomes

Change to table view

Actions taken since the breach or attack (where the incident had an outcome)	Businesses	Charities
Technical changes (such as updated antivirus software)	41%	39%
People or training changes (such as staff training or communications)	33%	45%
Governance changes (such as increased monitoring)	18%	22%
Any action taken	83%	89%
No action taken	14%	11%

Bases: Those that were able to specify a breach or attack experienced in the last 12 months and had an outcome: 175 businesses; 60 charities

Chapter 6: Cyber crime

This chapter covers cyber crime and the frauds that occur as a result of cyber breaches and attacks (cyber-facilitated fraud) [footnote 17]. It further explores the threat landscape for UK organisations, by establishing a subset of the number of cyber breaches or attacks that could be defined as crimes, in terms of the Computer Misuse Act 1990 and the Home Office Counting Rules.

The chapter covers:

- the prevalence of cyber crimes, 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
- estimates of the financial cost of cyber crime
- a similar set of statistics with regards to frauds that occur as a result of cyber breaches or attacks (cyber-facilitated fraud)

Some of the cyber security breaches and attacks reported in Chapter 4 do not constitute cyber crimes under the above definition. For example, some attempted attacks will not have penetrated an organisation's cyber defences and some, such as online impersonation, would be beyond the scope of the Computer Misuse Act. Therefore, the statistics on prevalence and financial cost of cyber crime differ from the equivalent estimates for all cyber security breaches or attacks (in Chapter 4). They should be considered as a distinct set of figures, specifically for crimes committed against organisations, so are a subset of all breaches and attacks.

The questions reported in this chapter allow us to monitor the prevalence of, and harm caused by, cyber crimes against organisations, using a similar approach to accredited official statistics estimates of crime against individuals from the general public Crime Survey for England and Wales (CSEW), and police-recorded crime. Both of these follow the Home Office Counting Rules, and are published in the Office for National Statistics Crime in England and Wales release (https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest).

It is important to remember that, as with all cyber security breaches and attacks, the survey can only measure cyber crimes or fraud that organisations can identify and recall. There are likely to be hidden crimes, and others that organisations cannot recall in detail, so the findings reported here may tend to underestimate prevalence and scale.

Key takeaways

- We estimate that 19% of businesses and 14% of charities have been the victim of at least one cyber crime in the last 12 months, accounting for approximately 267,000 businesses and 28,000 registered charities.
- The larger the business, the more likely they were to experience cyber crime (17% of micro businesses, 24% of small businesses, 41% of medium businesses and 48% of large businesses). The same pattern was evident among charities with likelihood to experience cyber crime increasing with income (10% of low-income charities, 18% of medium-income charities, and 34% of high-income charities).
- The prevalence of cyber crime has remained relatively stable for the last few years among businesses (22% in 2023/2024, 20% in 2024/2025 and 19% in 2025/2026) and charities (14% in all three years). There was also no change in non-phishing related cyber crime among both businesses (3% in 2023/2024, 4% in 2024/2025 and 3% in 2025/2026) and charities (2% in 2023/2024, 3% in 2024/2025 and 2% in 2025/2026).
- There may be signs of sector specific improvements, namely in the information and communication sector. Whilst prevalence of cyber breaches or attacks remained in line with last year (63% this year compared to 69% last year), the proportion of businesses in the sector experiencing a cyber crime has decreased by almost half (from 43% in 2024/2025 to 22% this year), suggesting that defences against the most serious cyber breaches or attacks could be strengthening in the information and communication sector.
- Phishing cyber crime remained by far the most common type of cyber crime experienced (93% of businesses and charities that experienced a cyber crime, 18% of all businesses and 13% of all charities).
- Whilst the prevalence of cyber crime overall remained static, for charities there was a decrease in hacking cyber crime among all charities (from 2% in 2024/2025 to 1% this year) and an increase in ransomware cyber crimes among all charities (from less than 0.5% in 2024/2025 to 1% this year).
- The median number of cyber crimes experienced in the last 12 months, was three cyber crimes for both businesses and charities. This remains roughly in line with last year where the median number experienced was four cyber crimes for both businesses and charities. Taking the mean estimates, businesses and charities both experienced 19 cyber crimes of any kind in the last 12 months. This data indicates a high level of repeat victimisation amongst some organisations experiencing cyber crime.
- Using mean number of cyber crimes[footnote 18] , it was estimated that UK businesses have experienced approximately 5.19 million cyber crimes of

all types including approximately 70,000 non-phishing cyber crimes in the last 12 months. UK charities have experienced approximately 525,000 cyber crimes of all types in the last 12 months.

- The median perceived cost of cyber crime other than phishing was £250, including those giving a cost of £0, and £750 excluding those giving a cost of £0. The top 10% of perceived costs (90th percentile) ranged from £5,000 for those including £0 costs to £7,500 for those excluding £0 costs. Whilst the majority of businesses are not experiencing extremely high costs associated with cyber crime, it is important to note that high cost cyber crime incidents do occur.
- For around 3% of businesses and 1% of charities, cyber breaches or attacks are seen to facilitate fraud, equating to approximately 43,000 businesses and 3,000 charities. There were an estimated 130,000 cyber-facilitated fraud events across the UK business population in the last 12 months.
- Among businesses experiencing cyber-facilitated fraud, including costs of £0, the median perceived cost was £110, and excluding those with a cost of £0, the median perceived cost was £500. The perceived cost in the top 10% of cases was £12,000 including those with a £0 cost and £15,000 when excluding £0 costs. This paints a similar picture to cyber crime costs, that whilst the majority of businesses do not experience very high costs associated with cyber-facilitated fraud, a minority of businesses do face high costs.

6.1 Note on comparability to previous year and official statistics status

The cyber crime questions in their current form were introduced in the 2023/2024 survey and therefore results since 2023/2024 are comparable with this year’s survey.

The exception is for cyber-facilitated fraud estimates and costs. Changes to the fraud questions in the 2024/2025 survey (to ask organisations to specifically include instances of fraud that were related to or as a result of phishing attacks) means that this year’s survey is only comparable to last year.

6.2 What constitutes crime

Cyber crime involves gaining unauthorised access, or causing damage, to computers, networks, data or other digital devices, or the information held

on those devices.

This survey covers multiple forms of cyber crime:

- ransomware attacks where a financial ransom was demanded
- hacking - unauthorised access of files or data, as well as online takeovers (e.g. of websites, social media accounts or email accounts and hacking of online bank accounts that did not lead to fraud) - that was carried out intentionally, including attacks that led to extortion
- denial of service attacks that breached an organisation's defences and were carried out intentionally, including attacks that led to extortion
- other computer viruses or malware that breached an organisation's defences
- phishing attacks that individuals engaged with (e.g. by opening an attachment) or that were targeted towards a specific organisation/recipient (e.g. containing personal data), and did not lead to any further crimes being committed

Sometimes multiple attack paths can be involved in one cyber incident, for example a phishing attack could lead to malware being installed on a device, which then allows the attacker unauthorised access to files. In order to adhere to the Home Office Counting Rules (https://www.gov.uk/government/publications/counting-rules-for-recorded-crime), and avoid double-counting of crimes, the survey asks respondents about each crime type in turn, in the order presented above (i.e. ransomware first, and phishing last). For each crime type, respondents are asked about any additional incidents that were separate to those already mentioned under the previous crime types. As a worked example, if an organisation experienced hacking that led to ransomware, and this breached their defences:

- we first ask about the ransomware attack
- we then establish that the ransomware attack constitutes a cyber crime (i.e. a financial ransom was demanded)
- we then ask the respondent to disregard that particular incident when being asked about further hacking attacks, so that the same crime is not counted twice

Cyber crime also facilitates other offences. In recognition of this, we have included questions that capture where cyber breaches or attacks have led to fraud (i.e. cyber-facilitated fraud). Cyber-facilitated fraud is deception to make a gain, or cause a loss, in relation to money, services, property or goods, which uses data or access obtained through cyber breaches or attacks. In these cases, to avoid double-counting, the incident is recorded here as a fraud rather than a cyber crime. We have included these fraud estimates to complement the cyber crime estimates. However, these cyber-

facilitated fraud statistics are not intended to capture all frauds committed against businesses, they only represent the frauds preceded by cyber breaches or attacks. Cyber-facilitated fraud is discussed separately in Sections 6.7 and 6.8. Cyber-facilitated fraud estimates are not included in any of the cyber crime estimates covered in Sections 6.3 to 6.6.

More details on the approach to this chapter can be found in the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report).

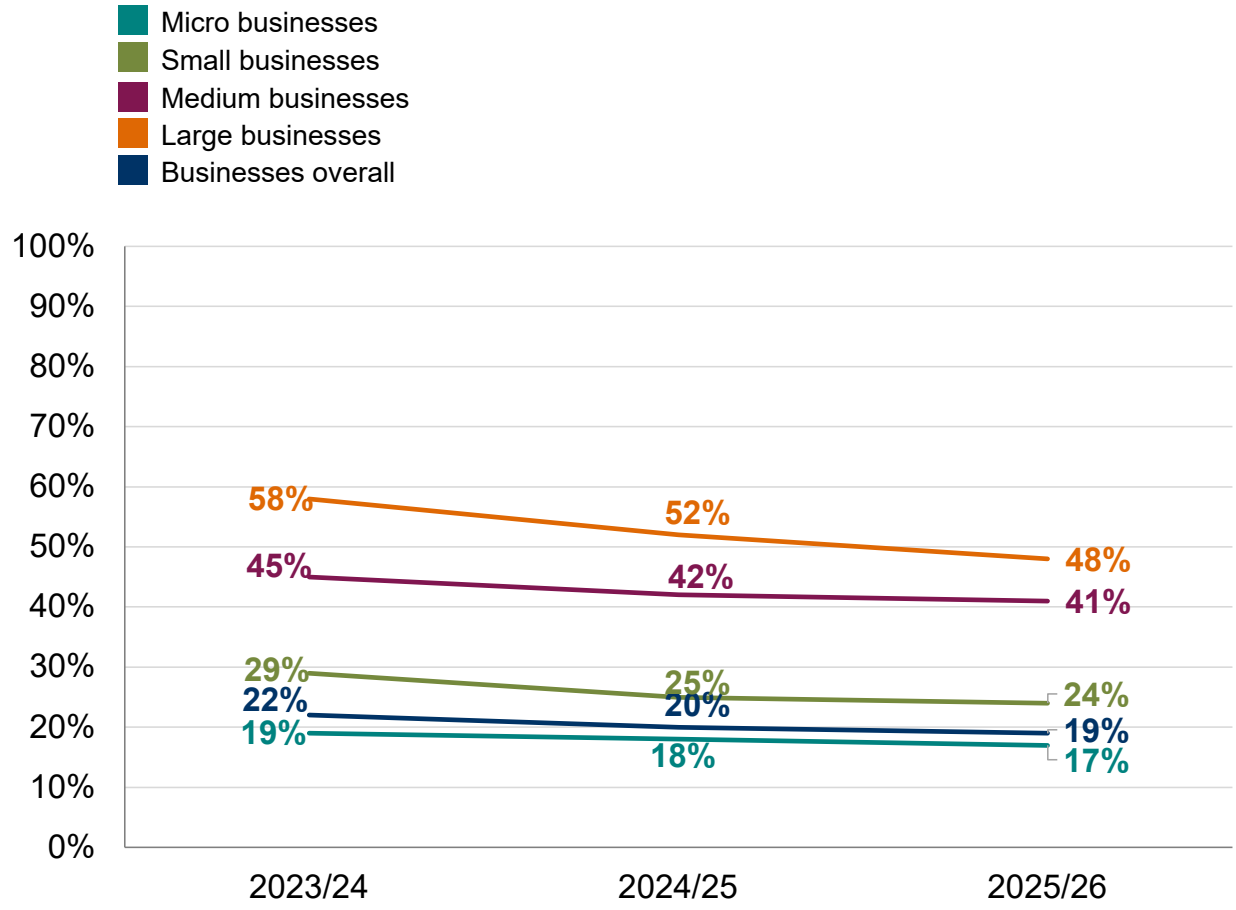
6.3 The prevalence of cyber crime

Looking across all the different types of cyber crime, we estimate that 19% of businesses and 14% of charities have been the victim of at least one cyber crime in the last 12 months. This accounts for approximately 267,000 businesses and 28,000 registered charities, although these estimates, like all survey results, will be subject to a margin of error (see Appendix A).

Looked at another way, among the 43% of businesses and 28% of charities identifying any cyber security breaches or attacks, just under half (44% of businesses and 49% of charities) ended up being victims of cyber crime.

As Figure 6.1 shows, across all businesses (i.e. not just those identifying breaches or attacks), the larger the business, the more likely they were to experience cyber crime. Whilst just under one in five micro businesses (17%) have experienced cyber crime in the last 12 months, the same was true for around a quarter of small businesses (24%), around two in five medium businesses (41%) and around half of large businesses (48%). This was similar to the trend for cyber security breaches and attacks more generally. As described in Chapter 4, the lower prevalence of cyber crime and cyber breaches and attacks among micro and small businesses compared to medium and large businesses may indicate poorer identification and reporting practices in smaller organisations, as they may have less sophisticated cyber security monitoring in place.

Figure 6.1: Percentage of businesses over time that have experienced any cyber crime in the last 12 months



bases 2025/26: 1,154 micro businesses; 507 small businesses; 296 medium businesses; 155 large businesses; 2,112 businesses overall
bases 2024/25: 1,013 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,179 businesses overall
bases 2023/24: 1,060 micro businesses; 506 small businesses; 264 medium businesses; 170 large businesses; 2,000 businesses overall

Figure 6.1 shows the prevalence of cyber crime among businesses overall and by business size over the last three years. Cyber crime prevalence does remain consistent with 2024/25 and 2023/24, with no statistically significant changes. However, a downward trend since 2023/24 can be observed, particularly among large businesses.

Looking at cyber crime experienced by business sector (Figure 6.2), those in the retail or wholesale sector were less likely to experience a cyber crime (12% compared to 19% businesses overall), echoing the fact they were also less likely to experience a cyber breach or attack (31% compared to 43% businesses overall).

There were no other significant differences by sector, which differed from last year where there was more variation by sector. In terms of changes over time by sector, this year the proportion of businesses in the information and communication sector experiencing a cyber crime decreased by almost half (from 43% in 2024/2025 to 22% in 2025/2026). The decrease in cyber crime among businesses in the information and communication sector has happened in spite of the prevalence of cyber breaches and attacks in this

sector remaining consistent (63% this year compared to 69% last year). This may suggest that defences against the most serious cyber breaches and attacks are strengthening in the information and communication sector.

Figure 6.2 : Percentage of businesses that have experienced any cyber crime in the last 12 months, by sector

Change to table view

Industry sector	
Administration or real estate	24%
Professional, scientific or technical	24%
Finance or insurance	23%
Information and communication	22%
Construction	21%
Health or social care	20%
Entertainment or service	20%
Utilities or production	17%
Food or hospitality	14%
Transport or storage	12%
Retail or wholesale	12%
Businesses overall	19%

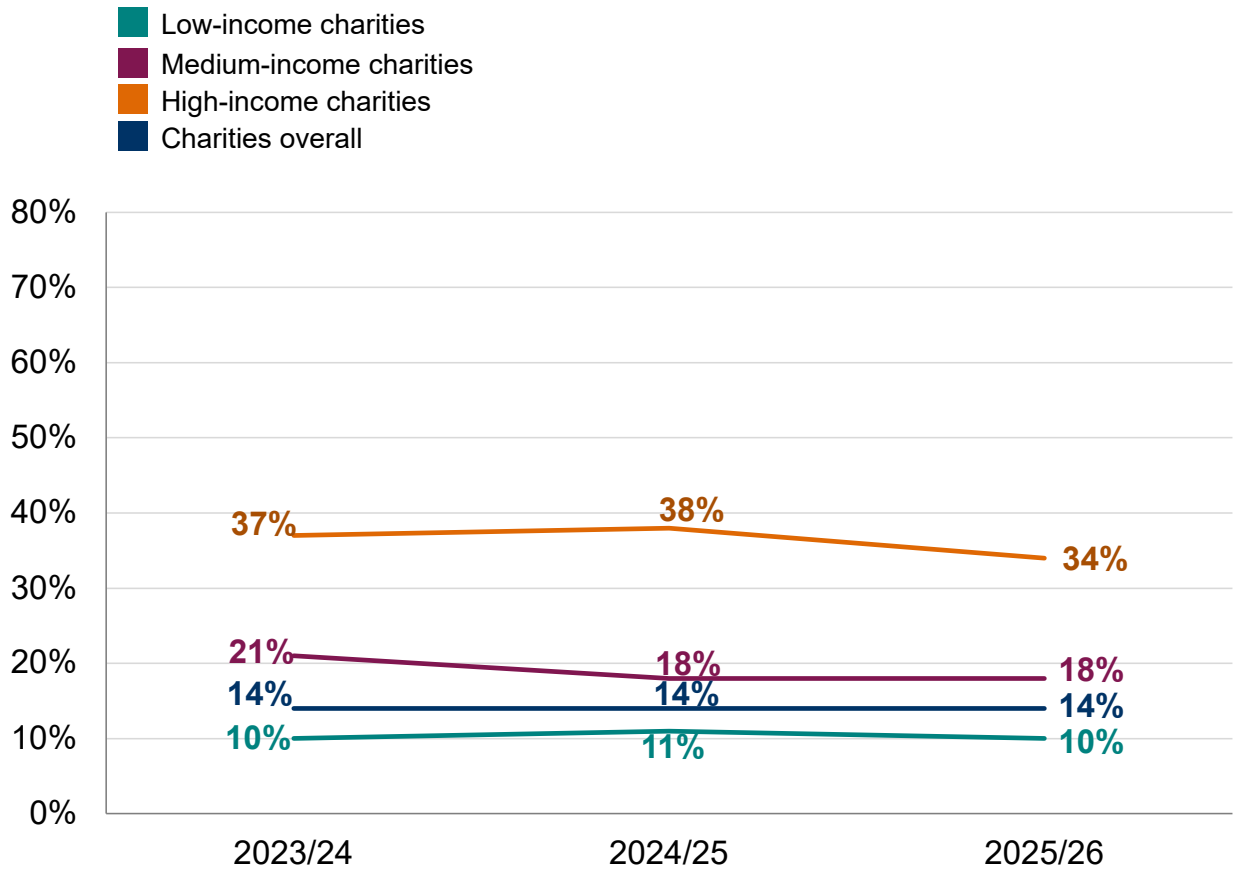
Bases: 81 information and communication businesses; 217 professional, scientific or technical businesses; 205 utilities or production businesses; 306 administration or real estate businesses; 262 construction businesses; 85 transport or storage businesses; 101 finance or insurance businesses; 163 entertainment or service businesses; 69 agriculture, forestry or fishing; 101 health or social care businesses; 184 food or hospitality businesses; 302 retail or wholesale businesses; 2,112 businesses overall

There was very little difference by region when looking at prevalence of cyber crime, however, reflecting the pattern with prevalence of cyber breaches and attacks, businesses in Northern Ireland were significantly less likely to experience a cyber crime (8% compared to 19% businesses

overall). While businesses in the London region experienced significantly more cyber crime than average last year (27% compared to 20% overall in 2024/25), it remained in line with businesses overall this year (20% of business in London and 19% of businesses overall). However, it is worth noting that regional analysis of prevalence will be influenced by other factors, such as the distribution of business sectors.

Looking at cyber crime prevalence by charity income, Figure 6.3 shows a similar pattern for cyber security breaches and attacks more generally, with charities likelihood to experience a cyber crime increasing with income (10% low-income charities, 18% medium-income charities, and 34% high-income charities).

Figure 6.3: Percentage of charities over time that have experienced any cyber crime in the last 12 months



Bases: 2025/26: 496 low-income charities, 254 medium-income charities, 335 high-income charities; 1,085 charities overall
Bases: 2024/25: 446 low-income charities, 292 medium-income charities, 343 high-income charities; 1,081 charities overall
Bases: 2023/24: 464 low-income charities, 205 medium-income charities, 335 high-income charities; 1,004 charities overall

There has been no significant change among charities, overall or within any income band (Figure 6.3) compared to 2024/2025 or 2023/2024.

The next section (Section 6.4) covers the types of cyber crimes that organisations faced. It is worth noting that most of the 19% of businesses and 14% of charities that identified any cyber crime are referring to phishing-related cyber crimes where individuals responded to a phishing email (e.g. by opening an attachment) or where the phishing email was targeted towards a specific organisation/recipient, but no other crime occurred as a result. When removing these phishing-related cyber crimes from the calculation, we estimate that a total of 3% of businesses and 2% of charities have experienced at least one non-phishing cyber crime in the last 12 months (in line with last year where 4% of businesses and 3% of charities experienced a non-phishing cyber crime). This amounts to approximately 38,000 businesses and 3,000 registered charities.

Similarly to all cyber crimes, non-phishing cyber crimes are more prevalent than average among large businesses (6% for large businesses compared with 3% of businesses overall) and medium and high-income charities (4% and 5% respectively compared with 2% of charities overall).

There has been a decrease in non-phishing cyber crimes observed this year among medium and large businesses. Whilst 4% of medium businesses experienced a non-phishing cyber crime this year, this was a decrease compared with 8% in 2024/2025. The most substantial drop was among large businesses compared to the previous two years (16% in 2023/2024 and 15% in 2024/2025 to 6% in 2025/2026). Despite this, no corresponding significant increase in phishing cyber crimes has been found among medium or large businesses.

6.4 The nature of cyber crimes experienced

Figure 6.4 details the types of cyber crimes that organisations have faced, among the 19% of businesses and 14% of charities that have been victim to at least one cyber crime.

Phishing cyber crime was by far the most common type of cyber crime experienced, with 93% of businesses and charities that experienced a cyber crime having experienced phishing. This equates to 18% of all businesses and 13% of all charities.

Hacking[footnote 19] was the second most common type of cyber crime, experienced by 8% of businesses and 4% of charities who experienced some type of cyber crime. This equates to 1% of all businesses and charities experiencing hacking cyber crime.

Ransomware cyber crime was experienced by 3% of businesses and 5% of charities who were the victim of a cyber crime (equating to 1% of all businesses and charities). Similar proportions experienced denial of service

cyber crime, 3% of businesses and 2% of charities who were the victim of a cyber crime (equating to less than 0.5% of all businesses and charities). Cyber crime relating to viruses, spyware or malware was experienced by 2% of businesses and 2% of charities who were the victim of a cyber crime (again equating to less than 0.5% of all businesses and charities).

Among businesses experiencing cyber crimes relating to unauthorised access, online takeovers or denial of service, 7% experienced some form of extortion, i.e. the attackers demanded a payment to end the breach or attack in question (not shown in Figure 6.4). While extortion does occur among organisations experiencing more serious forms of cyber crime, it represents a very small proportion of organisations overall. When considered across all businesses and charities, less than 0.5% experienced extortion of any kind (around 0.2% of businesses and 0.1% of charities), based on a very small number of cases.

Figure 6.4 : Percentage of organisations that have identified the following types of cyber crime in the last 12 months, among the organisations that have identified any cyber crime

Change to table view

Type	Businesses	Charities
Phishing attacks	93%	93%
Hacking (unauthorised access or online takeovers)	8%	4%
Ransomware	3%	5%
Denial of service	3%	2%
Viruses, spyware or malware	2%	2%

Bases: Those experiencing any cyber crime in the last 12 months: 511 businesses, 234 charities

There were a few regional differences when looking at the prevalence of cyber crime among all businesses (not just those experiencing a cyber crime). Businesses in the North West were more likely to experience hacking cyber crime (4% compared to 1% of businesses overall), businesses in the South East were more likely to experience a denial of service cyber crime (2% compared to less than 0.5% of businesses overall) and businesses in Wales were more likely to experience viruses, spyware or malware cyber crime (2% compared to less than 0.5% of businesses

overall). Again, it is worth noting that regional analysis of prevalence will be influenced by other factors, such as the distribution of business sectors.

We can estimate how many businesses and charities are affected by each type of cyber crime by extrapolating these results to the total business and charity populations. These estimates are shown in Table 6.1. Again, these estimates, like all survey results, are subject to a margin of error (see Appendix A).

Table 6.1: Extrapolations of businesses and charities that have experienced a cyber crime in the last 12 months, by type of cyber crime

Type of cyber crime	Number of businesses that experienced cyber crime	Number of charities that experienced cyber crime
Base	2,112	1,085
Phishing	248,000	26,000
Hacking	21,000	1,000
Ransomware	9,000	1,000
Denial of service	7,000	-
Viruses, spyware or malware	6,000	1,000

‘-’ denotes that for charities experiencing denial of service cyber crimes the estimate was too low to produce an extrapolation.

Trends over time

Prevalence of the different types of cyber crime has remained largely consistent with 2024/2025. The exception for businesses was for ransomware cyber crimes as a proportion of those businesses experiencing at least one cyber crime which decreased from 7% in 2024/2025 to 3% this year. This chimes with Chapter 4 where ransomware attacks among businesses were also seen to decline this year compared to the previous two years, both as a proportion of those experiencing breaches and attacks and all business. However, looking at ransomware cyber crimes as a proportion of all businesses there was no change between 1% in 2024/2025 and 1% this year.

For charities there have been two significant changes in the prevalence of cyber crime. There has been a decrease in hacking cyber crime among

charities experiencing cyber crime (from 17% in 2024/2025 to 4% this year) and among all charities (from 2% in 2024/2025 to 1% this year). Conversely, there has been an increase in ransomware cyber crimes both among charities experiencing cyber crime (from less than 0.5% in 2024/2025 to 5% this year) and among all charities (from less than 0.5% in 2024/2025 to 1% this year).

There were no other significant changes in type of cyber crime experienced between 2024/2025 and 2025/2026, either as a proportion of those who experienced cyber crime, or as a proportion of all businesses and charities.

6.5 The scale of cyber crime

Some organisations may be the victims of cyber crime multiple times. Our survey also estimated the scale of cyber crime, that is, the number of times cyber crime has occurred among the 19% of businesses and 14% of charities that identified any cyber crime in the last 12 months.

Looking at the number of cyber crimes experienced by organisation type (Figure 6.5) we see that whilst a third (33%) of businesses experiencing cyber crime only identified one cyber crime in the last 12 months, a sizeable minority were persistently targeted (20% experienced between 11 and 99 cyber crimes and 5% experienced 100 or more cyber crimes). The same was true for charities, where 23% of charities who identified a cyber crime in the last 12 months experienced between 11 and 99 cyber crimes and 4% experienced 100 or more cyber crimes.

Figure 6.5 : Number of cyber crimes identified by organisations who have experienced cyber crime in the last 12 months

Change to table view

Organisation Type	% 1 cyber crime	% 2-10 cyber crimes	% 11-99 cyber crimes	% 100+ cyber crimes	Total
Businesses	33	42	20	5	
Charities	34	40	23	4	

Bases: Those experiencing any cyber crime in the last 12 months: 511 businesses, 234 charities

Note: Figures may not sum to 100% due to rounding and percentage labels are not always shown for some small categories due to space

The median number of cyber crimes experienced in the last 12 months, which may be more reflective of the typical organisation, was three cyber crimes for both businesses and charities. This remains roughly in line with last year, where the median number experienced was four cyber crimes for both businesses and charities. Taking the mean estimates, businesses and charities both experienced 19 cyber crimes of any kind in the last 12 months.

This data indicates a high level of repeat victimisation amongst some organisations experiencing cyber crime. This was still the case when looking at non-phishing related crime, but to a much lesser extent. Among the 3% of businesses identifying non-phishing cyber crimes, the mean average was two and the median average was one.[footnote 20]

As the results are representative of the overall business and charity populations, it is possible to extrapolate from the mean results and present estimates for the scale of cyber crime across the overall UK business and charity populations. However, it should be noted that these population estimates will have an associated wide margin of error because sample sizes are based on the subset of businesses and charities that have experienced cyber crime. In addition, the mean number of cyber crimes is used to calculate these extrapolations and it should be noted that the mean is susceptible to skews from a small number of outliers that may be present in the data.

Using the results from this Cyber Security Breaches Survey 2025/2026, we estimate that:

- UK businesses have experienced approximately 5.19 million cyber crimes of all types
- UK charities have experienced approximately 525,000 cyber crimes of all types in the last 12 months

Looking at the scale of specific types of cyber crime, where base sizes allow[footnote 21], we estimate that:

- UK businesses have experienced approximately 5.13 million phishing cyber crimes in the last 12 months
- UK businesses have experienced approximately 70,000 non-phishing cyber crimes in the last 12 months
- UK charities have experienced approximately 523,000 phishing cyber crimes in the last 12 months

6.6 Financial cost of cyber crimes

Since 2022/2023, this survey series has attempted to capture the perceived cost of cyber crime on organisations[footnote 22].

This year, we have stopped reporting the mean costs. Given the distribution of cyber crime is highly skewed and subject to high sampling error this is not a robust statistical indicator. It can also create a disclosure risk where a dominant share of the total cost is from a limited number of organisations.

The median perceived cost is presented, as well as adding the 25th-75th percentile range where most cases fall, the top 10% of cases (90th percentile) and the top 5% of cases (95th percentile).

There has been a small change in the statistical methodology[footnote 23] used to calculate the median.

Table 6.2 shows the estimated perceived costs organisations incurred from all their identified cyber crimes over the past 12 months, excluding costs relating to phishing cyber crime (which was captured by the survey for the first time this year and is included in Table 6.3). Due to small sample sizes, it was not possible to break down these figures by the size of business (as was done with the cost estimates for cyber security breaches and attacks in Chapter 4), or by crime type. Similarly, the number of cases for charities experiencing non-phishing cyber crime was too low to report cost estimates. A proportion of businesses say that the cyber crimes they experienced incurred no cost. The estimates excluding them are effectively showing the cost of cyber crimes that have a material impact on the business.

Table 6.2 shows that the median perceived cost of cyber crime other than phishing was £250, including those giving a cost of £0, and £750 excluding those giving a cost of £0. The range where most perceived costs fell (25th to 75th percentile) was £0 to £3,000 including £0 costs and £250 to £5,000, excluding £0 costs. The top 10% of perceived costs ranged from £5,000 for those including £0 costs to £7,500 for those excluding £0 costs. These findings suggest that whilst the majority of businesses are not experiencing extremely high costs associated with cyber crime, a minority of businesses are experiencing high costs.

While the tables focus on median costs and percentile ranges to reflect the experiences of most organisations, it is important to note that high cost cyber crime incidents do occur. These incidents tend to be rare, highly variable in nature and often organisation specific, which makes them persistently difficult to measure robustly within a survey of this size. As a result, extreme costs are not always fully reflected in the headline statistics,

particularly where disclosure or reliability thresholds limit the reporting of upper percentiles.

Table 6.2: Distribution of perceived cost per business of all cyber crimes (excluding phishing) experienced in the last 12 months

	Businesses experiencing any cyber crime other than phishing (including those giving a cost of £0)	Businesses experiencing any cyber crime other than phishing (excluding those giving a cost of £0)
Median perceived cost	£250	£750
Range of perceived cost where most fall (25th to 75th percentile)	£0 to £3,000	£250 to £5,000
Perceived cost for the top 10% of cases (90th percentile)	£5,000	£7,500
Perceived cost for the top 5% of cases (95th percentile)	Effective base size under 50 - cannot report	Effective base size under 50 - cannot report
Base	63	44

Table 6.3 shows the distribution of cyber crime costs including costs associated with phishing cyber crime, which was included for the first time this year. The median perceived cost of all cyber crimes, including those giving a cost of £0, was £0 and excluding those giving a cost of £0, was £400. The range of perceived cost where most businesses fell (25th to 75th percentile) was also low, £0 to £0 for those including £0 costs, only increasing to £60 to £1,000 for those excluding £0 costs. This suggests that where phishing cyber crimes were taking place, they tended to be lower cost than other types of cyber crime, with the majority having no cost. This does not necessarily align with findings in Chapter 4, which identified perceptions of phishing as the most disruptive type of breach or attack. This warrants further exploration in future waves of the survey to understand the relationship between cost of phishing cyber crime and disruption.

Table 6.3: Distribution of perceived cost per business of all cyber crimes (including phishing) experienced in the last 12 months

	Businesses experiencing any cyber crime (including those giving a cost of £0)	Businesses experiencing any cyber crime (excluding those giving a cost of £0)
Median perceived cost	£0	£400
Range of perceived cost where most fall (25th to 75th percentile)	£0 to £0	£60 to £1,000
Perceived cost for the top 10% of cases (90th percentile)	£500	£5,000
Perceived cost for the top 5% of cases (95th percentile)	£3,000	£15,000
Base	501	131

6.7 Cyber-facilitated fraud

Prevalence of cyber-facilitated fraud
The questions to obtain cyber-facilitated fraud estimates were edited in 2024/2025 to specifically ask organisations to include fraud as a result of phishing attacks. On this basis we were unable to directly compare cyber-facilitated fraud estimates, including prevalence and cost, to any wave before 2024/2025.

A total of 3% of all businesses and 1% of all charities have been a victim of fraud that resulted from a cyber breach or attack in the last 12 months.

When extrapolating this to the business population, this equates to approximately 43,000 businesses and 3,000 charities.

Prevalence of cyber-facilitated fraud has remained stable over the last two years for both businesses and charities. In 2024/2025 and 2025/2026 3% of businesses experienced cyber-facilitated fraud, as did 1% of charities.

Scale of cyber-facilitated fraud
Amongst the 3% of businesses that experienced cyber-facilitated fraud, just under half (46%) said this happened just once in the last 12 months and around a quarter (23%) said it had happened twice. The average (mean) number of cyber-facilitated frauds experienced by these businesses was three per business, with the median equating to two cyber-facilitated frauds per business.

As with the scale of cyber crime estimates (see Section 6.5), it was possible to extrapolate from these results and present estimates for the overall business population. Once again, it should be noted that these will have an associated wide margin of error (based on a sample size of 73 businesses). Nevertheless, we estimate that there were approximately 130,000 cyber-facilitated fraud events across the entire business population in the last 12 months.

The sample size was too low (31)[footnote 24] to include the results (including any extrapolated population estimates) for charities.

The breaches or attacks preceding cyber-facilitated fraud
Figure 6.6 shows the cyber breaches and attacks that led to cyber-facilitated fraud. Among the 3% of businesses that fell victim to cyber-facilitated fraud, 45% said this resulted from a phishing attack and 40% said this resulted from hacking or attempted hacking of online bank accounts, consistent with last year. After phishing attacks and hacking, the most common enablers of cyber-facilitated fraud were takeovers of organisation's or user's accounts (14%) and unauthorised access of files or networks by people outside of the organisation (10%). It should be noted that these questions were dependent on respondents being able to identify the origins of the fraud, but we do not know how often or how accurately they were able to do this.

Figure 6.6 : Percentage of businesses that had specific breaches or attacks leading to cyber-facilitated fraud, among the businesses experiencing any cyber-facilitated fraud

Change to table view

Phishing attacks	45%
Hacking or attempted hacking of online bank accounts	40%

Takeovers or attempts to take over your website social media accounts or email accounts	14%
Unauthorised accessing of files or networks by people outside your organisation	10%
Unauthorised accessing of files or networks by staff or volunteers	6%
Malware other than ransomware (viruses or spyware)	5%
Unauthorised listening into video conferences or instant messaging	2%
Denial of service attacks*	0%

Bases: Businesses that experienced cyber-facilitated fraud in the last 12 months: 73
*0% estimates displayed here represent percentages greater than 0% but too small to be rounded up to 1%. We refer to these estimates in the text as “less than 0.5%”.

As noted in Section 6.2, our survey estimates for cyber crime and cyber-facilitated fraud were mutually exclusive. We do not double-count instances of cyber-facilitated fraud to be cyber crime as well. If criminal activities like targeted hacking led to fraud, they are counted as cyber-facilitated fraud. If they did not lead to fraud, i.e. if the targeted hacks did not lead to anything else, they are counted as cyber crimes.

6.8 Financial cost of cyber-facilitated fraud

Table 6.4 outlines the average perceived cost per business of all cyber-facilitated fraud experienced in the last 12 months. Again, the sample size was too low to include costs for charities.

Table 6.4: Distribution of perceived cost per business of all cyber-facilitated fraud experienced in the last 12 months

	Businesses experiencing any cyber-facilitated fraud (including those giving a cost of £0)	Businesses experiencing any cyber-facilitated fraud (excluding those giving a cost of £0)
Median perceived cost (midpoint or typical)	£110	£500

	Businesses experiencing any cyber-facilitated fraud (including those giving a cost of £0)	Businesses experiencing any cyber-facilitated fraud (excluding those giving a cost of £0)
Range of perceived cost where most fall (25th to 75th percentile)	£0 to £2,000	£150 to £5,000
Perceived cost for the top 10% of cases (90th percentile)	£12,000	£15,000
Perceived cost for the top 5% of cases (95th percentile)	Effective base size under 50 - cannot report	Effective base size under 50 - cannot report
Base	71	43

Among businesses experiencing cyber-facilitated fraud, including costs of £0, the median perceived cost was £110, with the range of perceived cost where most fell (25th to 75th percentile) ranging from £0 to £2,000. Among those who had a cost associated with cyber-facilitated fraud, the median perceived cost was £500, with the range of perceived cost where most fell (25th to 75th percentile) ranging from £150 to £5,000. The perceived cost in the top 10% of cases (90th percentile) was £12,000 including those with a £0 cost and £15,000 when excluding £0 costs. This paints a similar picture to cyber crime costs, that whilst the majority of businesses do not experience very high costs associated with cyber-facilitated fraud, a minority of businesses do face high costs.

Chapter 7: Conclusions

Despite some high-profile, disruptive cyber attacks of 2025/2026, the survey does not reveal any broader increasing trend in attacks or cyber crimes, nor a corresponding economy-wide shift in increased cyber resilience. Whilst in the main most organisations receive few attacks, and costs are relatively low, a minority do experience repeated attacks and in some cases extremely high impact costs. One might have expected the major incidents

at large and well-known organisations to spur a significant increase in vigilance, but cyber security prioritisation and action has not moved substantially, with long-standing issues like the resilience gap between large firms and SMEs persisting.

While broad trends are stable, including the prevalence of cyber breaches or attacks and cyber crime, the data reveals some specific areas of progress, some of which reverse previously concerning declines. Board-level responsibility for cyber security in businesses has seen a positive increase to 31% (from 27%), reversing a downward trend since 2020/2021. Similarly, after years of decline, awareness of the government's Cyber Aware campaign has increased among both micro-businesses (from 22% to 29%) and charities (from 26% to 30%). There is awareness of newer government schemes, such as the Cyber Governance Code of Practice, and the Software Security Code of Practice (both launched in 2025). Overall, 16% per cent of businesses and charities had heard of the former; 22% of businesses and 19% of charities had heard of the latter.

There may also be signs of sector specific improvements, namely in the information and communication sector. Whilst the prevalence of cyber breaches or attacks in the information and communication sector has remained consistent with last year, the proportion of businesses in the sector experiencing a cyber crime has decreased by almost half since 2024/2025. This suggests that defences against the most serious cyber breaches or attacks could be strengthening in the information and communication sector.

Even where some defences are improving, small businesses declined on a number of cyber hygiene measures after temporary increases last year. This included a decrease this year on the proportion of small businesses undertaking cyber security risk assessments, having a formal policy in place covering cyber security risks and having a business continuity plan that covered cyber security.

There was also a perception from the qualitative interviews that breaches, particularly related to phishing attacks, appeared to be growing in sophistication. Among those experiencing breaches or attacks, phishing is becoming ever more dominant, with an increase in phishing-only attacks among both businesses and charities. Findings suggest that the wider impact of cyber breaches and attacks and cyber crimes might also be growing, making them potentially more difficult for organisations to handle. This was particularly evident among micro-businesses, where the proportion able to recover from their most disruptive breach in less than a day fell from 92% to 86%. This increased difficulty in recovery, which is happening despite modest gains in technical controls, suggests that the nature of attacks is evolving. An increase in wider impacts such as loss of revenue and reputational damage was also observed among businesses.

In a year marked by a record number of high-profile incidents, and an increase observed in ransomware cyber crimes among charities, a critical gap in incident response planning presents a growing risk to UK organisations. Only 25% of businesses have a formal incident response plan. This means for the 43% of businesses that experienced a cyber breach or attack in the last year, most were forced to react without a pre-defined strategy.

There has been a significant decline in the frequency of cyber security updates provided to boards in medium businesses, with the proportion receiving at least annual updates falling from 78% to 70%. Among charities, the proportion deeming cyber security a high priority has decreased from 68% last year to 60% this year. This trend is concerning because less frequent board engagement limits the ability of security experts to influence strategy, secure investment, and drive the adoption of NCSC guidance. It suggests that despite cyber security being a stated priority, the sustained, high-level focus required to build true organisational resilience is waning.

Appendix A: Guide to statistical reliability

The final estimates from the survey are based on weighted samples, to represent the entire population of UK businesses or charities with employees. The estimates are therefore subject to margins of error, which vary with the size of the sample and the percentage figure concerned. Figures are most uncertain when respondents are equally likely to have or have not experienced something.

For example, for a question where 50% of the 2,112 businesses sampled in the survey give a particular answer, there is a 95% chance that this result would not be more or less than 2.6 percentage points higher or lower than the true figure that would have been obtained had the entire UK business population responded to the survey. The margins of error that are assumed to apply in this report are given in the following table.[footnote 25]

Tables A.1 Margins of error (in percentage points) applicable to percentages at or near these levels

	10% or 90%	30% or 70%	50%
2,112 businesses	±1.6	±2.4	±2.6
1,154 micro businesses	±1.9	±2.9	±3.1

	10% or 90%	30% or 70%	50%
507 small businesses	±2.8	±4.3	±4.7
296 medium businesses	±3.6	±5.6	±6.1
155 large businesses	±5.1	±7.8	±8.5
1,085 charities	±2.1	±3.2	±3.5

Following feedback in our recent review by the Office for Statistics Regulation, we will look to provide more uncertainty ranges within this statistical report.

Appendix B: Glossary

Broad definitions of cyber security terms

Term	Definition
Cyber security	Cyber security includes any 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.
Cyber attack	A cyber attack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation.
Cyber crime	In the context of this study, cyber crime involves gaining unauthorised access, or causing damage, to computers, networks, data or other digital devices, or the information held on those devices. Examples of cyber crime include hacking or unauthorised access into online accounts (e.g. banking, email or social media accounts), denial of service attacks, or devices being infected by a virus or other malicious software (including ransomware).
Cyber-facilitated	In the context of this study, we define fraud as being dishonest action, with the intent of making a financial gain at the expense

Term	Definition
fraud	of an organisation. Cyber-facilitated fraud is deception to make a gain, or cause a loss, in relation to money, services, property or goods, which uses data or access obtained through one or more of the following: ransomware viruses, spyware or malware; denial of service attacks; hacking (unauthorised access to devices, including computers, smartphones and other internet-connected devices, as well as online takeovers); phishing attacks.
Cyber security breach	A cyber security breach is any incident that results in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
Outcome	A negative outcome from a cyber security breach or attack involves a temporary or permanent material loss from an organisation, such as a loss of money or data.
Impact	A negative impact from a cyber security breach or attack does not have to involve a material loss. This could be issues relating to staff disruption or implementing new measures in the organisation.

Definitions of types of cyber security breaches

Term	Definition
Denial of service attack	Denial of service attacks try to slow or take down organisations' websites, applications or online services, to render these services inaccessible.
Hacking	In the context of this study, we define two forms of hacking. Firstly, unauthorised access of files or networks, or entry into video conferences or instant messaging. Secondly, online takeovers of organisations' websites, social media accounts or email accounts.
Malware	Malware (short for "malicious software") is a type of computer programme designed to infiltrate and damage computers without the user's consent (e.g. viruses, worms and Trojan horses).

Term	Definition
Phishing	Phishing involves fraudulent attempts to extract information such as passwords or personal data (e.g. through emails or by filling in forms on websites), or to install malware on the recipient's device or network. In the context of this study, we define phishing as staff receiving fraudulent emails, or arriving at fraudulent websites.
Ransomware	Ransomware is a type of malicious software designed to block access to a computer system until a sum of money (a ransom) is paid.
Social engineering	Social engineering involves manipulation of specific individuals to extract important information, such as passwords or personal data, from an organisation, for example, through impersonation.

Definitions relating to cyber security processes or controls

Term	Definition
Cloud computing	Cloud computing uses a network of external servers accessed over the internet, rather than a local server or a personal computer, to store or transfer data. This could be used, for example, to host a website or corporate email accounts, or for storing or transferring data files.
Digital Service Providers	Digital Service Providers (DSPs) manage a suite of IT services like an organisation's network, cloud computing and applications.
Patch management	Patch management is about software security being regularly or automatically patched. In the context of this study, we define it as organisations having a policy to apply software security updates within 14 days of them being made available.
Penetration testing	Penetration testing is where staff or contractors try to breach the cyber security of an organisation on

Term	Definition
	purpose, in order to show where there might be weaknesses in cyber security.
Removable devices	Removable devices are portable devices that can store data, such as USB sticks.
Restricting IT admin and access rights	This is where only certain users are able to make changes to the organisation's network or computer settings, for example to download or install software.
Software as a Service	Software as a Service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet.
Threat intelligence	Threat intelligence is where an organisation may employ a staff member or contractor or purchase a product to collate information and advice around all the cyber security risks the organisation faces.
Two-factor authentication	Two-factor authentication (2FA), or multi-factor authentication (MFA) is an electronic authentication method in which a user is granted access to a network or application only after successfully presenting two or more pieces of evidence to an authentication mechanism (e.g. a password and a one-time passcode).
Virtual Private Network	A Virtual Private Network (VPN) is an encrypted network connection, allowing remote users to securely access an organisation's services.

Definitions relating to business or charity characteristics

Term	Definition
Micro business	Businesses with 1 to 9 employees.
Small business	Businesses with 10 to 49 employees.
Medium business	Businesses with 50 to 249 employees.

Term	Definition
Large business	Businesses with 250 or more employees.
SME	Small to medium enterprise.
Low-income charity	Charities with an income of less than £100,000.
Medium-income charity	Charities with an income of £100,000 to £499,999.
High-income charity	Charities with an income of £500,000 or more.

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
- Tom Bristow, Ipsos
- Hannah Harding, Ipsos
- Jono Roberts, Ipsos
- Eva Radukic, Ipsos
- Jayesh Navin Shah, Ipsos

1. 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.
2. The lead DSIT analyst for this release is Emma Johns and the responsible DSIT statistician is Saman Rizvi. The Home Office responsible statistician for this release is Lamyr Megnin. For enquiries on this release, from an official statistics perspective, please contact DSIT at cybersurveys@dsit.gov.uk.
3. The Cyber Security Breaches Survey is an official statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https://www.statisticsauthority.gov.uk/code-of-practice/

(https://www.statisticsauthority.gov.uk/code-of-practice/). Details of the pre-release access arrangements for this dataset have been published alongside this release.

4. This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252.

---

1. How the extrapolations in this report have been calculated is included in Section 1.9 of the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report).
2. It should be noted that the mean is susceptible to skews from a small number of outliers that may be present in the data.
3. Fieldwork for the Cyber Security Breaches Survey took place between August and December 2025, where organisations were asked about their cyber security experiences over the preceding 12 months. This data is referred to as 2025/2026. Please see Section 1.5 for more information on the survey year naming convention.
4. Where mean scores or costs are compared, significance testing has not been carried out. The large range of answers in the data means that further statistical testing is needed to identify statistically significant differences. However, looking at the pattern of mean scores across subgroups, and the direction of travel from earlier surveys, can still generate valuable insights in these instances.
5. Subgroup differences highlighted are either those that emerge consistently across multiple questions or evidence a particular hypothesis (i.e., not every single statistically significant finding has been commented on).
6. Further detail on significance testing is included in the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-technical-report) in Section 1.8.
7. To note, these are private sector education businesses. Results for public sector schools, colleges and universities are covered in the separately published Education Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings).
8. This was the percentage of businesses and charities that say they have all of the following rules or controls: having network firewalls, security controls on company-owned devices, restricting IT admin and access rights to specific users, up-to-date malware protection, and a policy to apply software updates within 14 days.

9. Cyber crime as defined in reference to the Computer Misuse Act 1990 (https://www.legislation.gov.uk/ukpga/1990/18/contents) and the Home Office Counting Rules (https://www.gov.uk/government/publications/counting-rules-for-recorded-crime).
10. The survey does not have a separate question to ask whether organisations have experienced any type of breach or attack, as this approach would be subject to considerable recall errors. Instead, the above percentages are based on calculating the proportions of businesses and charities that identified one or more of 11 specific types of breaches or attacks (listed in Figure 4.4), as well as an option allowing organisations to state any other type of breach or attack.
11. The cost estimates throughout the report are rounded to the nearest £10. The mean and median scores exclude “don’t know” and “refused” responses. They merge together the answers from respondents who gave a numeric value as well as those who gave only a banded value (because they did not know the exact answer). For the latter, we have imputed numeric values from the given banded values. We lay out this approach in detail in the Technical Annex.
12. The open-source programming language R was used to calculate the median this year, compared with SPSS in previous years. This reflects a methodological change resulting from differences in how the two tools apply survey and frequency weights.
13. Following statistical disclosure control guidance by the ONS a minimum effective base size of 50 cases is needed to report on the 95th percentile.
14. Note that Action Fraud was renamed to “Report Fraud” on December 5th, 2026, a change that took place after the vast majority of fieldwork for CSBS 2025/2026 was already completed.
15. Since these interviews were conducted, Action Fraud has been replaced by a new service called Report Fraud. However, this report continues to reference Action Fraud to remain consistent with the terminology used in the interview questions.
16. Whether a cyber-facilitated fraud has taken place is derived from the questions in the survey asking about the breaches and attacks that have been experienced. Whether or not the breaches or attacks that led to fraud constituted a cyber crime is not verified. We therefore cannot explicitly say that cyber-facilitated fraud captured in the survey was as a result of a cyber crime. However, we hypothesise that the cyber breaches or attacks that led to fraud would have been successful, and therefore where a cyber-facilitated fraud has occurred, that it will most likely be as a result of cyber crime.
17. It should be noted that the mean is susceptible to skews from a small number of outliers that may be present in the data.

18. Wherever hacking is referred to throughout Chapter 6 it is referring to hacking including unauthorised access or online takeovers.
19. There were too few cases of non-phishing cyber crime among the sampled charities to report statistically reliable results.
20. Other types of cyber crime extrapolations on scale cannot be made due to insufficient base sizes of those experiencing the relevant cyber crime.
21. The cost estimates throughout the report are rounded to the nearest £10. The mean and median scores exclude “don’t know” and “refused” responses. They merge together the answers from respondents who gave a numeric value as well as those who gave only a banded value (because they did not know the exact answer). For the latter, we have imputed numeric values from the given banded values. We lay out this approach in detail in the Technical Annex.
22. The open-source programming language R was used to calculate the median this year, compared with SPSS in previous years. This reflects a methodological change resulting from differences in how the two tools apply survey and frequency weights.
23. After weighting was taken into account this equated to an effective base size of 18.
24. In calculating these margins of error, the design effect of the weighting has been taken into account. This lowers the effective base size used in the statistical significance testing. The overall effective base size was 1,376 for businesses (compared with 1,326 in 2024/2025, 1,398 in 2023/2024, 1,702 in 2022/2023 and 816 in 2021/2022) and 777 for charities (compared with 685 in 2024/2025, 652 in 2023/2024, 808 in 2022/2023 and 267 in 2021/2022).