GOV.UK

Department for Science, Innovation & Technology

Home Office

Official Statistics

Cyber security breaches survey 2025

Published 10 April 2025

Contents

This publication is available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

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 2024.

Lead analysts: Saman Rizvi (DSIT), Eleanor Fordham (Home Office)

Responsible statistician: Saman Rizvi

Enquiries: cybersurveys@dsit.gov.uk

Summary

Introduction

The Cyber Security Breaches Survey 2025, 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. 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.

Identification of cyber security breaches and attacks

Just over four in ten businesses (43%) and three in ten charities (30%) 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 61,000 UK charities that identified a cyber breach or attack in the past year[footnote 1]. This represents a decrease in prevalence among businesses compared to 2024 (where 50% experienced a breach or attack, equating to 718,000 businesses).

The decrease was primarily driven by fewer micro and small businesses identifying phishing attacks (35% of micro businesses down from 40% in 2024 and 42% of small businesses down from 49% in 2024). The prevalence of cyber breaches and attacks in medium and large businesses remains high (67% medium and 74% large) and was similar to 2024 (70% medium and 75% large).

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. Where cyber crimes are being referred to it is made explicit in the text.

Of businesses or charities that experienced a breach or attack in the last 12 months, phishing attacks remain the most prevalent and disruptive type of breach or attack (experienced by 85% of businesses and 86% of charities). The qualitative interviews highlighted that phishing attacks were often cited as time-consuming to address due to their volume and the need for investigation and staff training. The qualitative interviews also found that organisations had a growing consciousness that increasingly sophisticated methods, such as AI impersonation, were becoming mainstream.

While the proportion of organisations experiencing a negative outcome from a breach remained consistent with 2024, (16% of businesses and 16% of charities in 2025 compared to 13% of businesses and 12% of charities in 2024), specific outcomes show shifts. To note, the differences in these percentages were not statistically significant. Businesses reported a significant increase in temporary loss of access to files or networks (7%, up from 4% in 2024), while charities experienced a rise in loss of access to third-party services (5%, up from 1% in 2024).

Based on what respondents believed and self-reported, we estimated that the average cost of the most disruptive breach for each business in the last 12 months was £1,600 for businesses and £3,240 for charities. Excluding those who reported that the cost of their most disruptive breach was £0, the average cost of the most disruptive breach was £3,550 for businesses and £8,690 for charities. The costs reported here are self-reported estimates, which may represent an underestimation of full financial impact.

Cyber hygiene

Encouragingly, small businesses showed improvement in several cyber hygiene practices, including increased uptake of cyber security risk assessments (48%, an increase from 41% in 2024), cyber insurance (62% up from 49% in 2024), formal cyber security policy covering cyber security

risks (59% up from 51% in 2024), and business continuity plans that address cyber security (53% up from 44% in 2024).

Conversely, high-income charities showed a decline in several key areas compared to 2024, including activities to identify cyber security risks (75% down from 86% in 2024), reviewing immediate supplier risks (21% down from 36% in 2024), and having a formal cyber security strategy in place (39% down from 47% in 2024). Insight from the qualitative interviews suggest this could be linked to budget constraints.

A formal cyber security strategy was in place for seven in ten large businesses (70%) and significantly fewer medium businesses (57%).

The majority of businesses and charities have implemented basic technical controls, such as updated malware protection (77% businesses and 64% charities), password policies (73% businesses and 57% charities), network firewalls (72% businesses and 49% charities), backing up data securely via a cloud service (71% businesses and 58% charities) and restricted admin rights (68% businesses and 68% charities). However, adoption of more advanced controls like two-factor authentication (40% businesses and 35% charities), a virtual private network for staff connecting remotely (31% businesses and 20% charities) and user monitoring (30% businesses and 31% charities) remains lower than other measures.

Staff training and awareness raising activities on cyber security were more prevalent in large businesses (76% compared to 19% businesses overall). Whilst a consistent increase among large businesses on this measure was observed in recent years, the proportion of large businesses in 2025 remains in line with 2024 (74%).

Risk management and supply chains

Whilst the proportion of businesses overall conducting risk assessments (29%) has remained in line with 2024 (31%), as noted above, small businesses have seen a significant increase in those carrying out risk assessments covering cyber security (48% in 2025, up from 41% in 2024).

Charities at the overall level carrying out at least one activity to identify cyber risks has remained consistent with last year (42% in 2025 and 40% in 2024), however, as noted above, the proportion of high-income charities doing at least one of the activities has declined (from 86% in 2024 to 75% in 2025).

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 (14%) and under one in ten were looking at their wider supply chain (7%). 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, with around a third of medium businesses (32%) and nearly half of large businesses (45%) reviewing the cyber security risks posed by their immediate suppliers, in comparison to 11% of micro business and 21% of small businesses.

Almost half of businesses (45%) and a third of charities (34%) reported being insured against cyber security risks in some way. As in previous years, small and medium businesses were more likely than businesses overall (45%) to have some form of cyber insurance (62% small businesses and 65% medium businesses).

Board engagement and corporate governance

Cyber security remains a high priority for the majority of businesses (72%) and charities (68%), consistent with previous years. However, a trend has emerged as board-level responsibility for cyber security has steadily declined among businesses since 2021 (38% of businesses had a board member with responsibility for cyber security in 2021, compared to 27% in 2025).

Larger organisations demonstrated a higher prioritisation of cyber security (92% of medium businesses and 96% of large businesses) compared to businesses overall (72%).

Cyber accreditations and following guidance

While the overall proportion of organisations seeking external information or guidance on cyber security remained stable (42% of businesses and 37% of charities), large businesses demonstrated a decrease on this measure (51%, down from 67% in 2024).

Reliance on external cyber security consultants and IT providers remained the most common source of information (25% of businesses and 17% of charities), highlighting a potential gap in organisations' use of accessible and trusted guidance from official sources like the NCSC (National Cyber Security Centre) (1% of businesses and 2% of charities mentioned the NCSC by name).

Recognition of NCSC campaigns, such as Cyber Aware, were higher than NCSC by name, with Cyber Aware the most commonly recognised government communications initiative (24% of businesses and 26% of charities were aware). Despite this, there has been a steady decline in awareness of the Cyber Aware Campaign since 2021 (when 34% of businesses and 38% of charities were aware of it). Awareness of the 10 Steps guidance (12% of businesses and 15% of charities), and Cyber Essentials (12% of businesses and 15% of charities) was lower still, also reflecting a longer-term decline in awareness of the 10 Steps since 2020 (19% of businesses and 27% of charities) and Cyber Essentials since 2022 among businesses (16%). Limited awareness was particularly notable among micro businesses (22% were aware of Cyber Aware, 9% were aware of the 10 Steps guidance and 9% were aware of Cyber Essentials).

Incident response

Internal reporting to senior management remains the most common action following a breach or attack (76% of businesses and 80% of charities inform directors or trustees of the incident). External reporting remains uncommon, with only a third of organisations (32% of businesses and 30% of charities) having guidance on when to report a cyber breach or attack externally.

Larger organisations and those in sectors like health or social care, finance or insurance, and information or communication demonstrated a more formal approach to incident response, with higher adoption of incident response plans and documented procedures (53% of medium businesses, 75% of large businesses, 66% in the health or social care sector, 50% in the finance or insurance sector, 43% in the information or communication sector had an incident response plan).

Small businesses showed a significant increase in implementing various incident response measures compared to 2024, including guidance on internal reporting (55% compared to 48% in 2024), external communication plans (29% compared to 21% in 2024), and guidance on external reporting (48% compared to 41% in 2024).

Additional staff training or communications emerged as the most common preventative measure adopted following a breach (32% of businesses and 38% of charities), perhaps highlighting organisations' understanding of the importance of ongoing education and awareness raising.

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 20% of businesses and 14% of charities have been victims of at least one cyber crime in the past year, accounting for approximately 283,000 businesses and 29,000 charities. Looked at another way, among the 43% of businesses and 30% of charities identifying any cyber security breaches or attacks, just under half (46% of businesses and 48% of charities) ended up being victims of cyber crime.

The larger the business, the more likely they were to experience cyber crime (18% of micro businesses, 25% of small businesses, 43% of medium businesses and 52% of large businesses). The same pattern was evident among charities with likelihood to experience cyber crime increasing with income (11% of low-income charities, 18% of medium-income charities, and 38% of high-income charities).

The prevalence of cyber crime overall among businesses and charities remained consistent with 2024 (20% of businesses in 2025 and 22% of businesses in 2024 and 14% in both years for charities), as did non-phishing related cyber crime for businesses (4% in 2025 and 3% in 2024) and charities (3% in 2025 and 2% in 2024).

Whilst the prevalence of cyber crime overall remained static, the prevalence of ransomware among businesses has significantly increased between 2024 and 2025. The estimated percentage of all businesses who experienced a ransomware crime in the last 12 months increased from less than 0.5% in 2024 to 1% in 2025, which equates to an estimated 19,000 businesses in 2025.

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

Businesses who were victims of cyber crime experienced an average of 30 cyber crimes of any kind in the last 12 months, whereas for charities this was 16. For both business and charities the median was 4 cyber crimes. This indicates a high level of repeat victimisation amongst organisations experiencing cyber crime.

It is estimated that UK businesses have experienced approximately 8.58 million cyber crimes of all types including approximately 680,000 non-phishing cyber crimes in the last 12 months. UK charities have experienced approximately 453,000 cyber crimes of all types in the last 12 months.

The average self-reported cost per business associated with cyber crime (excluding phishing) experienced in the last 12 months was a mean average of £990 including £0 responses (and £1,970 excluding £0 responses).

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 40,000 businesses and 2,000 charities. There were an estimated 72,000 cyber-facilitated fraud events across the UK business population in the last 12 months.

Self-reported costs associated with cyber-facilitated fraud were higher than for cyber crime (cyber crime does not include cyber-facilitated fraud), with an estimated mean average cost per business of £5,900 including those giving a £0 response (and £10,000 excluding £0 responses).

Chapter 1: Introduction

1.1 Code of practice for statistics

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

1.2 Background

Publication date: 10 April 2025

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[footnote 2]. 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 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 2024 survey but remain broadly consistent this year. This means cyber crime results this year can be compared against 2024 but not against 2023. Changes to questions related to cyber-facilitated fraud mean that we are unable to directly compare cyber-facilitated fraud results this year to 2024 or 2023. Full details of all questionnaire changes between years are available in the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-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 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, staff training and responsibilities and governance
- 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 publication follows previous surveys in this series[footnote 4], published annually since 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-2025/cyber-security-breaches-survey-2025-education-institutions-findings).

1.3 Methodology

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

- Between August to December 2024, we undertook a random probability telephone and online survey of 2,180 UK businesses, 1,081 UK registered charities and 574 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 December 2024, to gain further qualitative insights from some of the organisations that answered the survey.

Sole traders and public-sector organisations 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-2025/cyber-security-breaches-survey-2025-education-institutions-findings), comprise 250 primary schools, 240 secondary schools, 52 further education colleges and 32 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-2025/cyber-security-breaches-survey-2025-technical-report).

1.4 Changes since the 2024 survey

The core approach for the 2025 study - data collected from organisations via a random-probability survey, predominantly conducted by telephone, was unchanged from the previous years. As such, we were 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 and 2025, there were some changes to the questionnaire. Key changes included:

- Wording modifications at the questions on fraud to ensure that phishing attacks that led to instances of fraud were adequately captured.
- Minor wording modifications at the questions on ransomware to increase the specificity of answers by changing the language from asking about 'successful' attacks that overcame internal or third-party software, to asking about 'attacks where a financial ransom was demanded'.
- Adding new questions on why no cyber insurance was held (among those that did not have it), what role cyber security had in purchasing new software and a follow up question for those that selected phishing attacks as the most disruptive attack (asking why it was the most disruptive).

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-2025/cyber-security-breaches-survey-2025-technical-report).

1.5 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 5] results, differences have been highlighted[footnote 6] only where statistically significant (at the 95% level of confidence)[footnote 7]. 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 is 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%" in charts with an accompanying note, and referred to as less than 0.5% in the text.

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 1.7 of the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-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 8]
- health or social care (Q)
- entertainment, service, or membership organisations (R and S)
- finance or insurance (K)
- food or hospitality (I)

- information or communications (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 is 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 2023 survey onwards, for businesses and charities, we substantially increased the use of split-sampling where certain questions are only asked to a random half of the sample 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.

1.6 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

- During the past 12 months, cyber security remained a high priority for around seven in ten businesses (72%) and charities (68%), in line with the previous two years.
- Around three in ten businesses (27%) and charities (30%) had board members or trustees taking explicit responsibility for cyber security as part of their job, and this was higher among larger businesses (66%). Whilst compared to last year the proportion of businesses remained stable (30% in 2024), it has been in steady decline since 2021 (38%).
- Whilst the proportion of businesses overall seeking external information or guidance remained stable (42% businesses compared to 41% businesses in 2024 and 37% charities compared to 39% charities in 2024), fewer large businesses were seeking external guidance than in the previous year (67% in 2024 compared to 51% in 2025).
- The most common source of information and guidance was external cyber security consultants, IT consultants or cyber security providers (25% businesses and 17% of charities), and this was highest among small (37%) and medium businesses (43%) and high-income charities (53%).
- Awareness of the Cyber Aware campaign (24% businesses and 26% charities), the 10 Steps guidance (12% businesses and 15% charities)

and Cyber Essentials (12% businesses and 15% charities) remained in line with 2024 for both businesses and charities. However, a longer-term decline in awareness amongst both is observed from 2021, and for businesses this was predominantly driven by a decline in awareness among micro businesses.

2.1 Perceived importance of cyber security

Around seven in ten businesses (72%) and charities (68%) reported that cyber security was a high priority for their senior management (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 is seen as a high or low priority for directors, trustees, and other senior managers

Organisation type	% Very High	% Fairly High	% Fairly Low	% Very Low	% Don't Know
Businesses	34	38	19	8	1
Charities	32	35	20	11	1

Bases: Split-sample half A: 1,046 businesses, 558 charities

It was more common for larger businesses to say that cyber security was a high priority (96% 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% medium businesses and 2% large businesses). The same was true for charities, where high-income charities were more likely to see cyber security as a high priority (88% of charities with an income of £500,000 or more compared with 68% of charities overall). This continued the pattern observed since 2020, where larger organisations tended to treat cyber security more seriously.

Businesses in the following sectors tended to treat cyber security as a higher priority than businesses overall:

- finance or insurance (97% said it was a high priority)
- utilities or production (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)

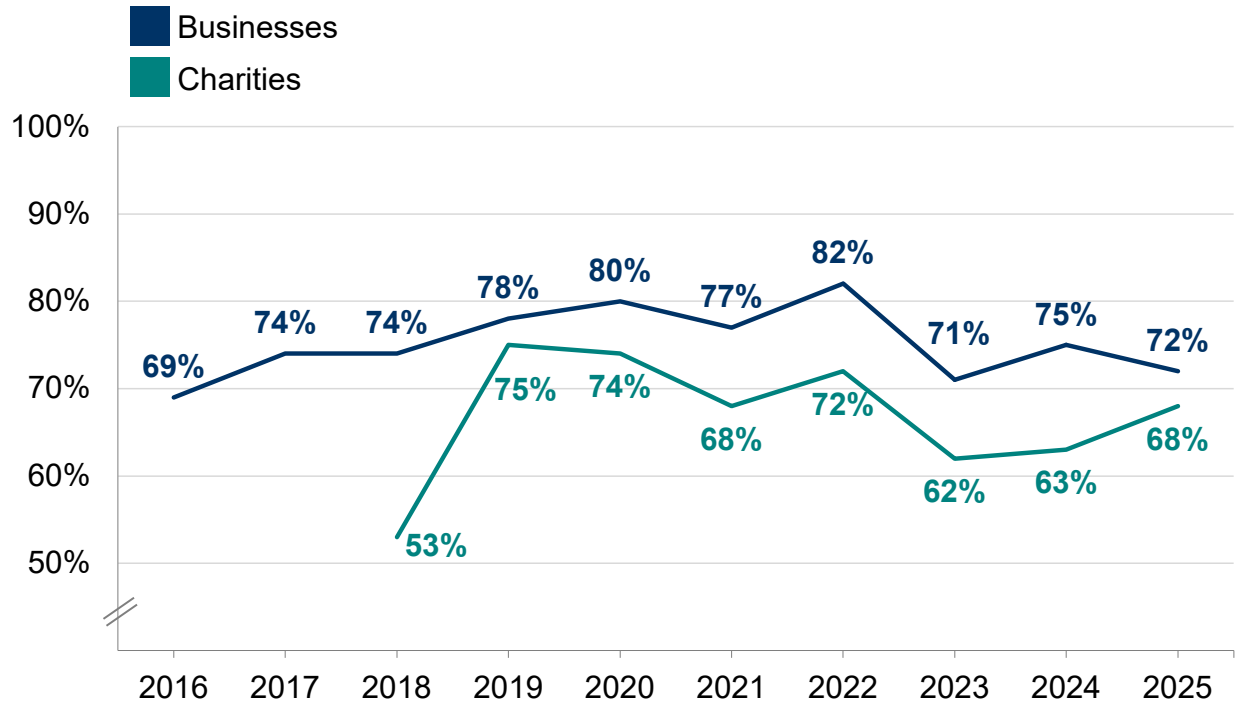
Conversely, and as seen in previous years, businesses in the retail or wholesale sector tended to regard cyber security as a lower priority than those in other sectors (44% said it was a low priority compared with 27% of businesses overall).

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 remained in line with the previous two years (2024 and 2023).

Whilst the proportion of charities viewing cyber security as a high priority had not significantly increased this year, the decline in those rating it a high priority between 2022 and 2023 looks to be reversing and the gap between businesses and charities has become smaller than in the previous few years.

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



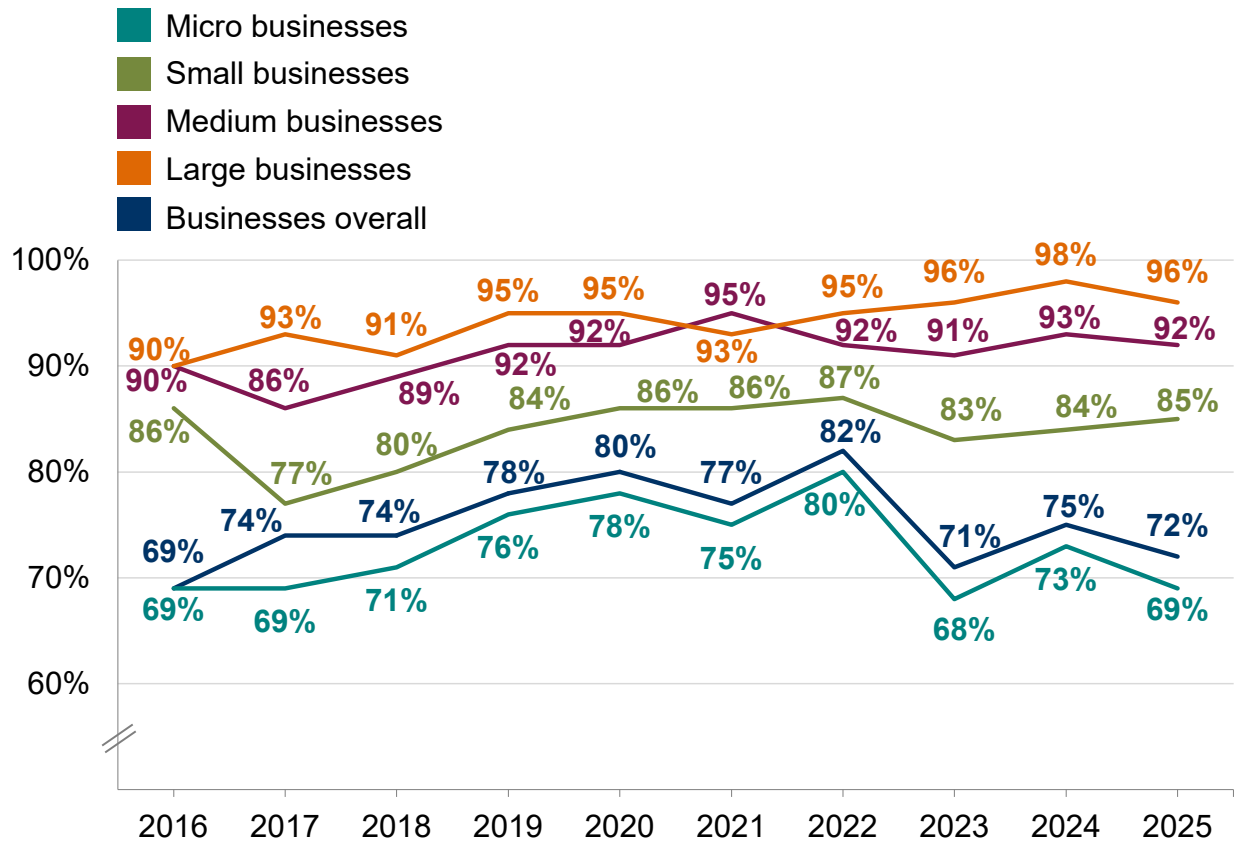
Bases: c.1,000+ businesses per year; 450+ charities per year (split sample half A from 2023 onwards)

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

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).

There have been no significant changes by business (Figure 2.3), or charity (Figure 2.4) size, compared to 2024. However, there has been a significant increase in the proportion of low-income charities who saw cyber security as a high priority (64% in 2025) when compared to 2023 (53%).

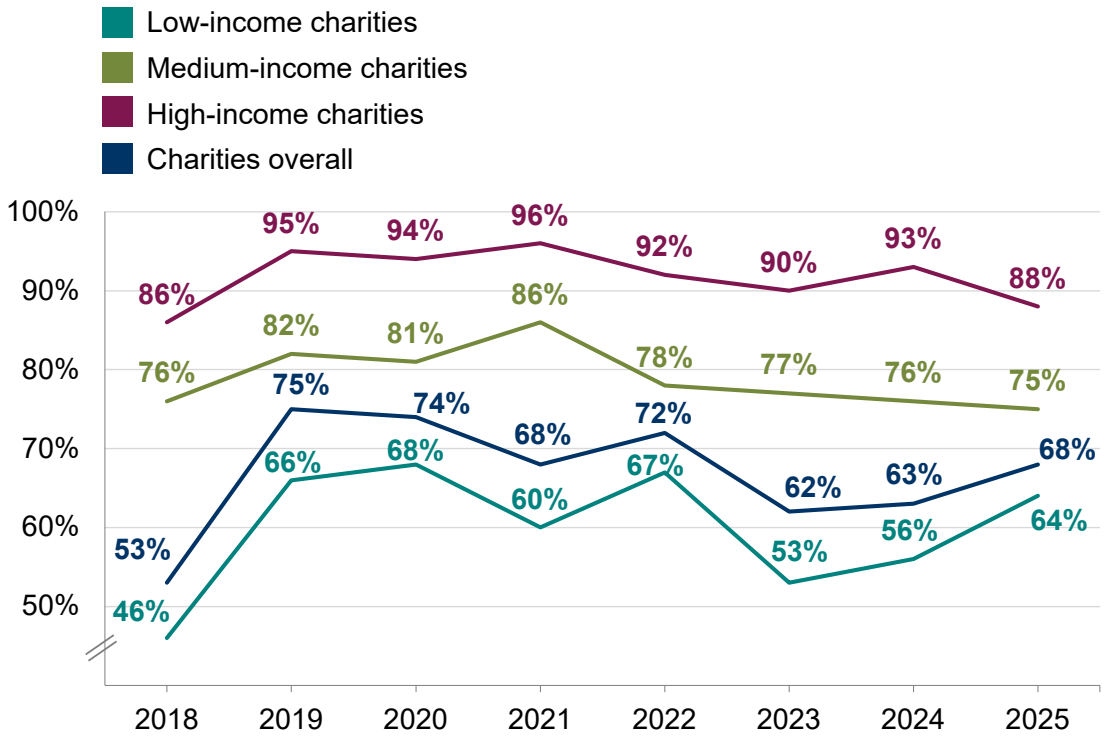
Figure 2.3: Percentage of businesses, by size, over time where cyber security is seen as a high priority for directors, trustees, and other senior managers



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 2023 onwards)

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

Figure 2.4: Percentage of charities, by size, over time where cyber security is 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 2023 onwards)

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

Qualitative insights on cyber security prioritisation

The qualitative interviews suggested that organisations were sensing a growing and more sophisticated cyber security threat and were aware there are processes and systems they need to have in place to meet that threat.

> "The world's changing and it's getting harder to control the risk really on cybersecurity. So we're trying to be a bit of ahead of the curve." **Quality and IT manager, Medium business**

> "[Our cyber security infrastructure has] improved since our last year. We've been focusing on that. Last year, the focus was on updating hardware, and now with the hardware sorted, it allows us to implement

> better cyber security protocols, which we've been doing over the last year." **IT & Digital Services Manager, Charity**

However, cyber security budgets for organisations typically remained flat and in some cases becoming more constrained, particularly among charities. This meant that despite a sense that cyber security should be an increasing priority, given growing concern over more sophisticated cyber security threats, organisations were not always able to translate this into action.

> "As many charities, I think we have been a bit more constrained in the last 12 months. There's definitely closer scrutiny of the bottom line and of budgets." **Director of Finance and Resources, Charity**

In some organisations there was a recognition that cyber security was a key area to invest in, and they did have intentions to better fund it, despite feeling hampered by the current budget.

> "We're looking at investing more resources in cyber security and that's both an additional manpower resource within the charity that's being considered and also a dedicated budget." **Data And Insight Manager, Charity**

> "Once we get the easy bits and pieces out of the way, we're going to have to start looking at things like theme tools and other software which is a lot more expensive and will need more investment." **Cyber Architect, Medium business**

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 2023, and results show that updates tend to be more frequent in businesses than in charities, continuing a trend from previous years.

Just over six in ten medium businesses (63%) and just over eight in ten large businesses (83%) updated their senior team at least quarterly, as did

just under six in ten high-income charities (57%)[footnote 9]. This remained consistent with findings in 2024.

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

Business type	% At least monthly	% Quarterly	% Annually	% Less than once a year	% Each time there is a breach or attack	% Never
Medium businesses	39	23	16	3	4	6
Large businesses	55	28	7	1	2	0
High-income charities	17	40	21	5	5	6

Bases: 413 medium businesses; 188 large businesses; 343 high-income charities

Board responsibilities

Just under three in ten businesses (27%) and the same 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, and while all registered charities have boards of trustees, not all businesses have a formal management board.

As might be expected, board-level responsibility was much more common in larger businesses, where the management board was likely to be larger. Two-thirds of large businesses (66%) had a board member responsible for cyber security compared with 27% of businesses overall.

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

Micro businesses	24%

Small businesses	42%
Medium businesses	51%
Large businesses	66%
Businesses overall	27%
Charities overall	30%

Bases: 1,014 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,180 businesses overall; 1,081 charities overall

As shown in Figure 2.7, businesses in the finance or insurance (57%), information or communications (52%) and professional, scientific or technical (36%) sectors were each more likely than businesses overall to have board members taking responsibility for cyber security. These sectors were the ones that were also most likely to prioritise cyber security (Section 2.1), and this is a trend that has been seen in previous years of the survey. At the other end of the scale, businesses in food or hospitality (12%) and construction (18%), were among the least likely to have board members assigned to this role, as were businesses in the retail or wholesale sector (22%), who were also less likely to be seen prioritising cyber security than other sectors.

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

Finance or insurance	57%
Information or communications	52%
Professional, scientific or technical	36%
Utilities or production	35%
Health or social care	34%
Administration or real estate	33%
Transport or storage	26%
Retail or wholesale	22%

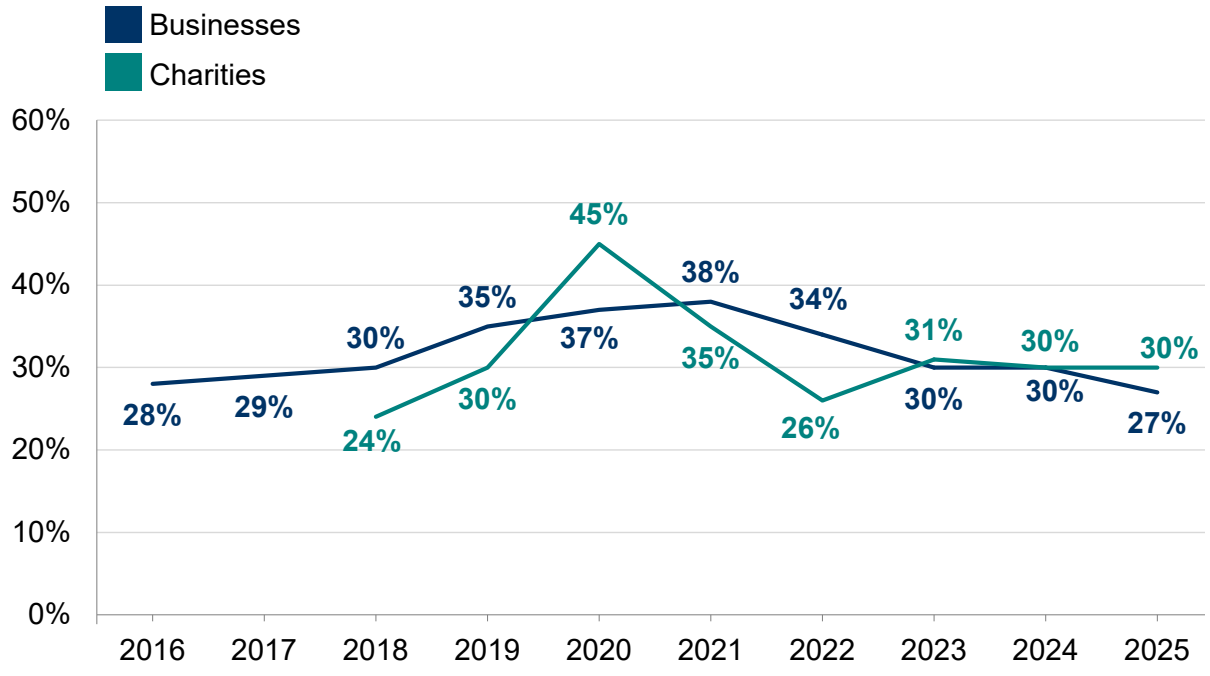
Entertainment or service	19%
Construction	18%
Food or hospitality	12%
Businesses overall	27%

Bases: 141 finance or insurance businesses; 130 information or communications businesses; 273 professional scientific or technical businesses; 150 utilities or production businesses; 94 transport or storage businesses; 357 retail or wholesale businesses; 100 entertainment or service businesses; 232 construction businesses; 168 food or hospitality businesses; 2,180 businesses overall

Trends over time

Figure 2.8 shows the trend over time for board members having specific cyber security responsibilities. The proportion this year remained stable for businesses and charities. However, the proportion of board members responsible for cyber security among businesses has seen a steady decline since 2021.

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

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

Qualitative insights on formal versus informal board engagement
Interest in cyber security at the board level was broadly seen as becoming more sustained and central to organisational strategy, rather than being treated as an incidental concern. Businesses and charities frequently mentioned that there was a constant dialogue between board members and staff members surrounding cyber security decisions.

> "[The board is] very involved, they don't give full autonomy to us to do whatever we want. We need to have a constant dialogue of this is what we're doing, this is why we're doing it." **IT & Digital Services Manager, Charity**

> "Nothing gets approval without first going to them [the board] and saying, this is exactly what it will do, what it will mean, what it is, how the money will be spent." **Cyber Architect, Medium business**

As seen in previous years, the qualitative interviews suggested that individuals taking day-to-day responsibility for cyber security highly valued engagement from senior board members. Senior engagement helped them secure the buy-in of wider staff, for example, when cyber security directives came with the backing of senior management they were found to have better up take and to be more likely to be adhered to. Senior buy-in was also a motivating factor to those responsible for cyber security to improve their own approaches, and furthermore it helped with getting quicker approval for new measures.

The findings suggested that the larger the organisation the more likely that board engagement was structured and formal. Larger organisations were observed having regular cyber security reports going to the board or having cyber security as a standing agenda item at board meetings (or at a subcommittee level just below the board). It was also typical for cyber security to be reviewed as part of a regular look at their risk register.

> "We produce a monthly metrics report that goes up to exec committee and the board, and then twice a year I present to our audit and risk committee." **Head of Cyber Security, Large business**

By contrast, in smaller organisations, the approaches for keeping boards informed tended to be more informal. Several of these interviewees

mentioned discussing cyber security with senior managers in a reactive or ad hoc manner, for example, only when a specific issue arose.

> "If there was an issue, I'd go to them if it needed a decision, but other than that, no, they're not really overly involved." **Head of Cyber Security, Charity**

Often, in these cases, it was clear that boards were placing a great deal of trust either in their internal IT leads, or in their external IT providers. They assumed that any serious issues would be flagged by them. It was also observed among some of the smaller businesses interviewed that the responsibility of cyber security was being passed onto external contractors. This sometimes resulted in senior managers disengaging from the topic and often failing to understand the actions being taken, both internally and externally.

However, board involvement in cyber security did not necessarily equate to cyber security expertise. Businesses and charities frequently mentioned that only one or two board members appeared to possess any technical knowledge of cyber security, and in some cases the board member with responsibility for cyber security had little understanding of it. This is an important knowledge gap because board members may be making decisions, such as on budgets, without realising the full extent of their impacts.

> "My chief exec said yesterday they've just done a cyber skills audit of the board and out of 12, only three said that they were 'understanding things'. So there's a weakness on the board from that perspective." **Director of finance and resources, Charity**

> "They recognise that they are not the experts in the field but recognise their place in making the right decisions to support the work that needs to be done." **Head of IT and systems, Charity**

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. Around four in ten businesses (42%) and charities (37%) reported

actively seeking information or guidance on cyber security from outside their organisation in the past year (Figure 2.9).

Small (56%) and medium (69%) businesses were most likely to seek out external information, as were medium-income charities with an income of between £100,000 and £500,000 (46%) and high-income charities with an income of £500,000 or more (71%).

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

Micro businesses	38%
Small businesses	56%
Medium businesses	69%
Large businesses	51%
Businesses overall	42%
Charities overall	37%

Bases: Split-sample half A: 491 micro businesses; 269 small businesses; 189 medium businesses; 97 large businesses; 1,046 businesses overall; 558 charities overall

At the overall level results were in line with 2024 (41% businesses and 39% charities), although for businesses the proportion seeking external information or guidance remained lower than it was in 2023 (49%) and 2022 (48%). For large businesses there has been a significant decline in the proportion seeking external information this year (51% in 2025, down from 67% in 2024).

Figure 2.10 highlights the proportion of businesses in each sector seeking external information and guidance. Businesses in the information or communications and professional, scientific or technical sectors were more likely to have sought external information or guidance (63% and 52% respectively). Businesses in the food or hospitality sector (25%) and the retail or wholesale sector (27%) were less likely than businesses overall (42%) 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

Information or communications	63%
Professional, scientific or technical	54%
Utilities or production	52%
Finance or insurance	49%
Administration or real estate	44%
Construction	38%
Entertainment or service	33%
Retail or wholesale	27%
Food or hospitality	25%
Businesses overall	42%

Bases: Split-sample half A: 73 information or communications businesses; 145 professional, scientific or technical businesses; 68 utilities or production businesses; 63 finance or insurance businesses; 156 administration or real estate businesses; 110 construction businesses; 45 entertainment or service businesses; 172 retail or wholesale businesses; 73 food or hospitality businesses; 1,046 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 25% of businesses and 17% of charities)
- internal sources within the organisation such as colleagues, in-house experts and the management board (5% of businesses and 9% charities)
- any government or public sector source, including government websites, regulators, and other public bodies (3% of businesses and 5% charities)
- general online searching (3% 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.

A wide range of individual sources were mentioned, with relatively low proportions for each. For example, just 1% of businesses and 2% of

charities mentioned the National Cyber Security Centre (NCSC) by name, in line with 2023 and 2024, however, recognition of NCSC campaigns, such as Cyber Aware, were higher (explored later in this Chapter). Among charities, fewer than one in twenty (3%) mentioned charity-specific sources such as their relevant Charity Commission. This highlighted that organisations were not going to official sources for advice and were instead more likely to rely on IT consultants.

There were a small number of further differences by size and between businesses and charities that should be noted, particularly around the use of external cyber security consultants, IT consultants or IT service providers:

- seeking information and guidance from external consultants or providers was most common among small (37%) and medium businesses (43%, significantly higher than among large businesses, 29%), continuing the pattern from previous years. It reflects that these businesses may recognise the need for more cyber security expertise, but had to procure it externally, rather than employing experts internally like many large businesses (18% use internal sources compared to 5% of businesses overall)
- among micro businesses, the most common sources were also external security/ IT consultants (22%), with the next most common responses being online searching (3%) and their bank's IT staff (3%)
- high-income charities were significantly more likely than average to see information and guidance from external consultants or providers (53%).

Awareness of government guidance, initiatives, and communications
The question around information sources in the previous subsection tends to under-represent actual awareness of government communications on cyber security, as it is asked unprompted for individuals doing the telephone survey. In these kinds of unprompted questions, individuals often do not recall specific things they have seen and heard. We therefore asked organisations, in a later set of prompted questions, whether they had heard of specific government initiatives or communications campaigns before. These included:

- the national Cyber Aware (http://www.cyberaware.gov.uk/) communications campaign, which offers tips and advice to protect individuals and small businesses against cyber crime
- the 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security) guidance, which summarises how organisations can protect themselves by managing cyber risk
- the government-endorsed Cyber Essentials (https://www.cyberessentials.ncsc.gov.uk/) scheme, which enables organisations to be certified independently for having implemented technical good-practice in cyber security

Cyber Aware was the most commonly recognised of these, with 24% of businesses and 26% of charities were aware (Figure 2.11 and 2.12). Just over one in ten businesses were aware of each of the 10 Steps to Cyber Security (12%) and Cyber Essentials (12%). Among charities, 15% were aware of the 10 Steps to Cyber Security and 15% were aware of the Cyber Essentials scheme.

Small, medium and large businesses continued to be significantly more aware of these initiatives:

- 47% of large businesses, 41% medium businesses, 33% small businesses and 22% micro businesses had heard of Cyber Aware
- 36% of large businesses, 31% medium businesses, 20% small businesses and 9% micro businesses were aware of the 10 Steps guidance
- 51% of large businesses, 43% medium businesses, 23% small businesses and 9% micro businesses were aware of Cyber Essentials

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

- 39% of high-income charities had heard of Cyber Aware compared to 26% of charities overall
- 29% of high-income charities were aware of the 10 Steps guidance compared to 15% of charities overall
- 40% of high-income charities were aware of Cyber Essentials compared to 15% of charities 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**

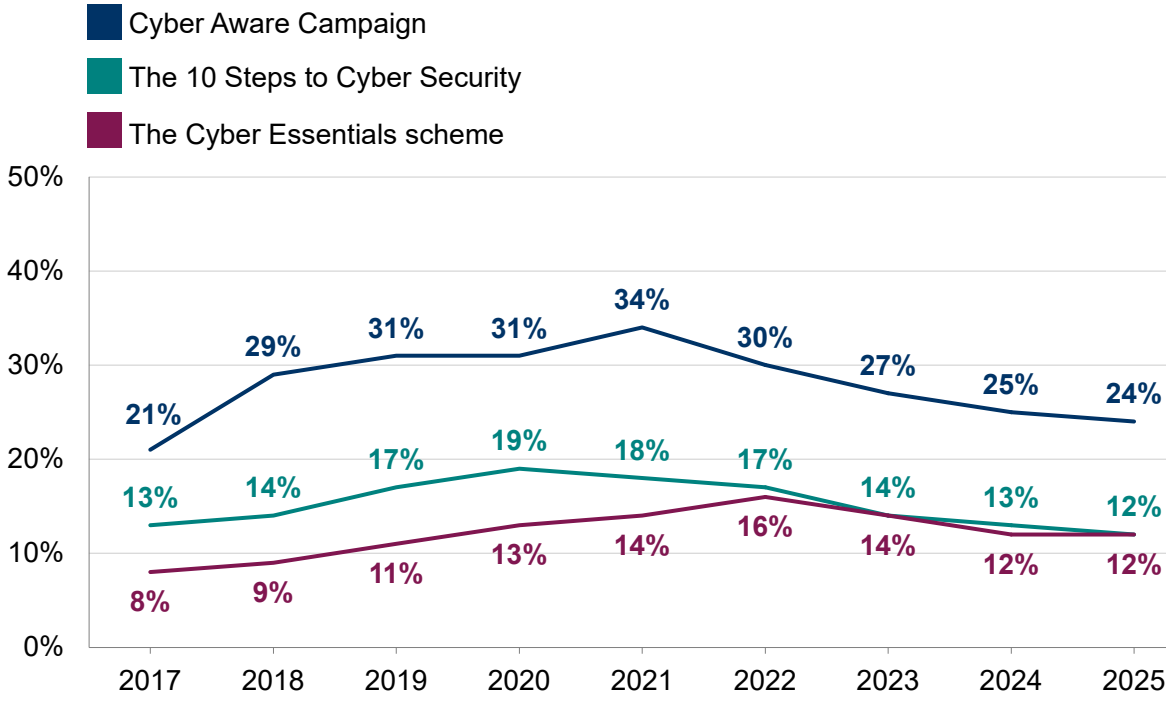
Some participants suggested that the NCSC should continue its current efforts but also exercised caution to avoid government advice saturation. Similarly, businesses did not always trust that government systems were completely secure, which raised some concerns around not always being able to trust that government guidance is 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 3 years. Looking further back (these questions in their current form were introduced in 2017) however, there has been a steady decline in awareness of the Cyber Aware Campaign since 2021.

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



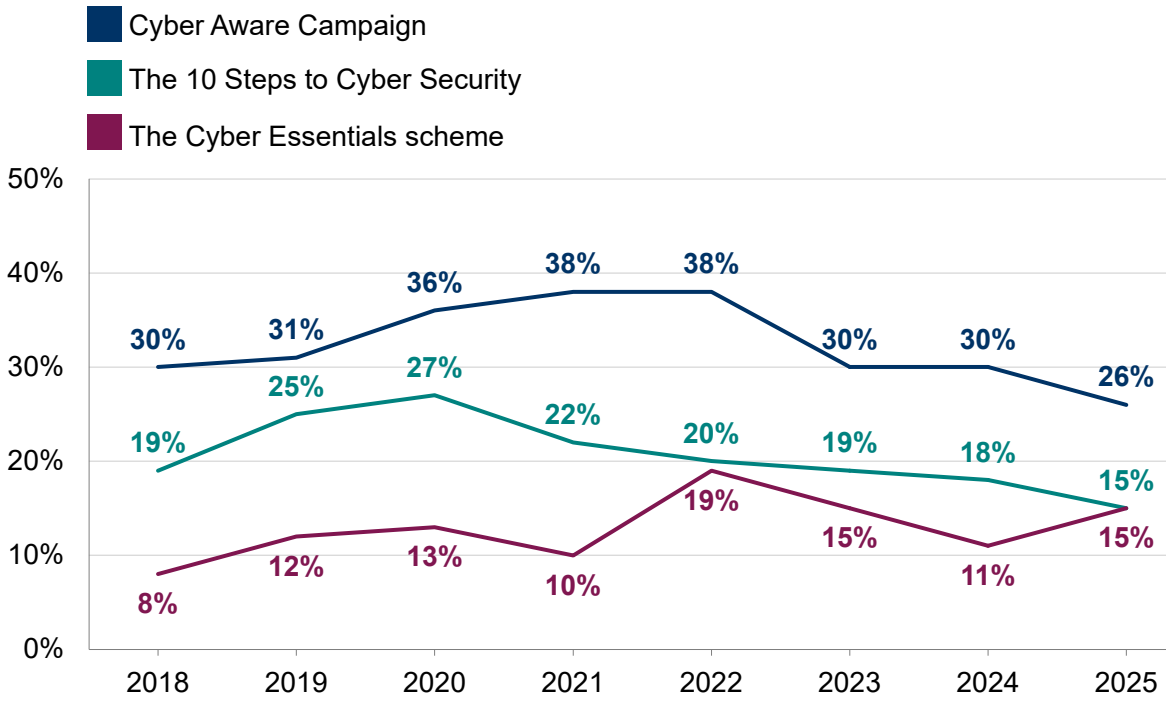
Bases: c.1,000+ businesses per year (split-sample half B from 2023 onwards)

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

The overall decline in awareness of the Cyber Aware campaign since 2021 was predominantly driven by a decline in awareness among micro businesses (from 34% in 2021 to 22% in 2025).

Charities have also seen longer term decline in awareness of the Cyber Aware campaign and the 10 Steps guidance (Figure 2.12), but awareness of all initiatives remains in line with 2024.

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 2023 onwards)

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

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

- the NCSC's Small Business Guide (https://www.ncsc.gov.uk/collection/small-business-guide) and Small Charity Guide (https://www.ncsc.gov.uk/collection/charity), which outline more basic steps that these smaller organisations can take to protect themselves
- the NCSC's Board Toolkit (https://www.ncsc.gov.uk/collection/board-toolkit), which helps management boards to understand their obligations, and to discuss cyber security with the technical experts in their organisation.

Awareness of any of the Small Business Guides (such as the Small Business Guide to Cyber Security and the Small Business Guide to Response and Recovery) among micro and small businesses continued to be stable but low (11% micro and 14% small in 2025 compared to 11% micro and 13% small in 2024).

Around one in seven charities (15%) had heard of the Small Charity Guide, but this was higher for medium (20%) and high-income charities (33%). The result for charities overall has been relatively consistent across years (15% in 2025 and 14% in 2024), however awareness among high-income charities has tended to fluctuate over the last few years. Awareness dropped significantly among high-income charities between 2023 and 2024 (from 36% to 21%), but has gone back up this year, a significant increase from 21% in 2024 to 33% in 2025.

The Board Toolkit was specifically explored with medium and large businesses in the survey, as well as high-income charities (from the 2022 study onwards). Around a fifth of medium businesses (22%), just over a quarter of large businesses (27%) and just under a fifth of high-income charities (17%) were aware of the Toolkit. This remains in line with previous years (when 23% medium businesses, 33% large businesses and 22% of charities were aware).

Impact of government information and guidance

Overall, 38% of businesses and 46% of charities recalled seeing at least one of the government communications or guidance covered in the previous section when prompted. This was consistent with 2024. Those aware of at least one form of government guidance were then asked about any changes they had made to their cyber security measures as a result of what they had seen. Around half of these businesses (48%) and charities (52%) reported making at least one change after seeing government guidance on cyber security, in line with 2024.

The proportion acting on seeing government initiatives or campaigns was higher for large (61%), medium (56%) and small (55%) businesses (compared with 44% of businesses overall). It was also higher for high-income charities (71% compared with 52% of charities overall).

In terms of the specific changes made, there were a wide variety of unprompted responses given. No single response appeared that frequently. The most frequent changes mentioned were:

- 28% of businesses and 29% of charities that recalled seeing at least one of the government communications reported making changes of a technical nature (e.g. to firewalls, malware protections, user access or monitoring) after seeing them.
- 20% of businesses and 20% of charities that saw government guidance said they had made changes regarding staffing (e.g. employing new cyber security staff), outsourcing or training.
- 12% of businesses and 23% of charities had made governance-related changes (e.g. increased spending, or updated policies or documentation). This represented an increase among charities compared to 2024 (14%). This was predominantly driven by an increase in new or updated cyber policies (from 4% of charities that had seen some government guidance

in 2024 to 10% in 2025) and new procurement processes for IT (1% of charities that had seen some government guidance in 2024 to 8% in 2025).

The top unprompted individual response categories were:

- staff training and communications (12% businesses and 10% charities).
- changing or updating firewalls or system configurations (10% businesses and 8% charities).
- new or updated antivirus software (8% businesses and 10% charities).
- outsourced cyber security/hired external provider (8% businesses and 7% 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 (including supplier risks)
- reporting cyber risks
- cyber insurance
- technical controls
- training and awareness raising
- staffing and outsourcing
- governance approaches and policies

We then 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

Small businesses have seen increases on a number of cyber hygiene measures, including:

- a rise in those undertaking cyber security risk assessments (48% up from 41% in 2024)

- an increase in those having cyber insurance in place, either from a specific cyber insurance policy or as cover from a wider insurance policy (62% up from 49% in 2024)
- a rise in both having a formal policy covering cyber security risks (59% up from 51% in 2024) and having a business continuity plan that covers cyber security in place (53% up from 44% in 2024)
- an increase in those with an external cyber security provider (62% up from 56% in 2024) - whilst not necessarily an indicator of cyber hygiene, for smaller businesses who typically do not have in house IT departments, it shows that cyber security is being taken seriously.

Whilst charities overall have remained consistent with last year on the majority of measures relating to approaches to cyber security, high-income charities look to have declined on a number of measures compared to 2024. This includes:

- the proportion deploying activities to identify cyber security risks (75% down from 86% in 2024), reviewing immediate supplier risks (21% down from 36% in 2024) and having a formal cyber security strategy in place (39% down from 47% in 2024).
- Around seven in ten large businesses (70%) and just under six in ten medium businesses (57%) have a cyber security strategy in place, consistent with 2024 (66% large businesses and 58% medium businesses).
- The majority of businesses (89%) and charities (82%) have undertaken key actions associated with at least one of the 10 Steps. However, while the proportion of charities doing so remains in line with 2024 (82%), the proportion of businesses is lower than in 2024 (94%).
- Whilst a small minority of businesses hold Cyber Essentials (3%), it is higher among larger businesses (21%), and the level of controls in place suggest that medium and large businesses, in particular, are potentially already meeting the Cyber Essentials standard, but not seeking certification.

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 shows the six key actions asked about in the survey. Deploying security monitoring tools and undertaking risk assessments continue to be the most common actions undertaken by both businesses and charities.

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

Activities	Businesses	Charities
Any of the listed activities	49%	42%
Used specific tools designed for security monitoring	30%	24%
Risk assessment covering cyber security risks	29%	29%
Tested staff (e.g. with mock phishing exercises)	18%	14%
Carried out a cyber security vulnerability audit	15%	13%
Penetration testing	12%	9%
Used or invested in threat intelligence	9%	6%

Bases: 2,180 businesses; 1,081 charities

Larger organisations were more likely to carry out these actions (92% of large businesses have carried out at least one of the actions, as have 84% of medium businesses and 75% of high-income charities), compared to 49% of businesses overall and 42% of charities overall.

The proportion of businesses deploying at least one these activities has remained consistent with 2024 (49% in 2025 and 51% in 2024). Whilst businesses overall have seen no change in the proportion conducting risk assessments covering cyber security risks (29% in 2025 and 31% in 2024), small businesses have seen a significant increase in those carrying out risk assessments covering cyber security (48% in 2025, up from 41% in 2024).

Charities at the overall level carrying out at least one of the activities have also remained consistent with last year (42% in 2025 and 40% in 2024). However, the proportion of high-income charities doing at least one of the activities has declined (from 86% in 2024 to 75% in 2025).

How organisations undertake audits and implement their findings
Among the 15% of businesses that undertook cyber security vulnerability audits, 23% carried out an internal audit only and 41% an external audit only. A third of businesses undertaking vulnerability audits (32%) 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 (44% micro businesses, 38% small businesses, and 38% 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 (54%).

A similar proportion of charities have carried out cyber security vulnerability audits (13%) compared to businesses (15%), however, contrary to the average business, the charities undertaking audits continued to be most likely do them solely on an internal basis only (33% compared to 23% of businesses). Around three in ten charities conducted both internal and external audits (30%) and external only audits (28%).

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 (14%) and under one in ten were looking at their wider supply chain (7%). Among charities, the respective figures were slightly lower (9% looked at their immediate suppliers and 4% at their wider supply chain).

As Figure 3.2 shows, there was extensive variation by size of organisation which is consistent with previous years. Possibly reflecting a more complex supply chain, around a third of medium businesses (32%) and nearly half of large businesses (45%) reviewed the cyber security risks posed by their immediate suppliers, in comparison to 11% of micro business and 21% of small businesses. It was still relatively rare for medium and large businesses to review their wider supply chain (15% and 25% respectively do so).

The proportion of charities overall reviewing immediate supplier risks (9% in both 2024 and 2025) has remained consistent, but there has been a significant decrease amongst high-income charities (36% in 2024 and 21% in 2025). Additionally, only 6% of these high-income charities have reviewed

their wider supply chains, which is also significantly lower than in 2024 (15%).

Figure 3.2: Percentage of organisations that have carried out work to formally review the potential cyber security risks presented by the following groups of suppliers

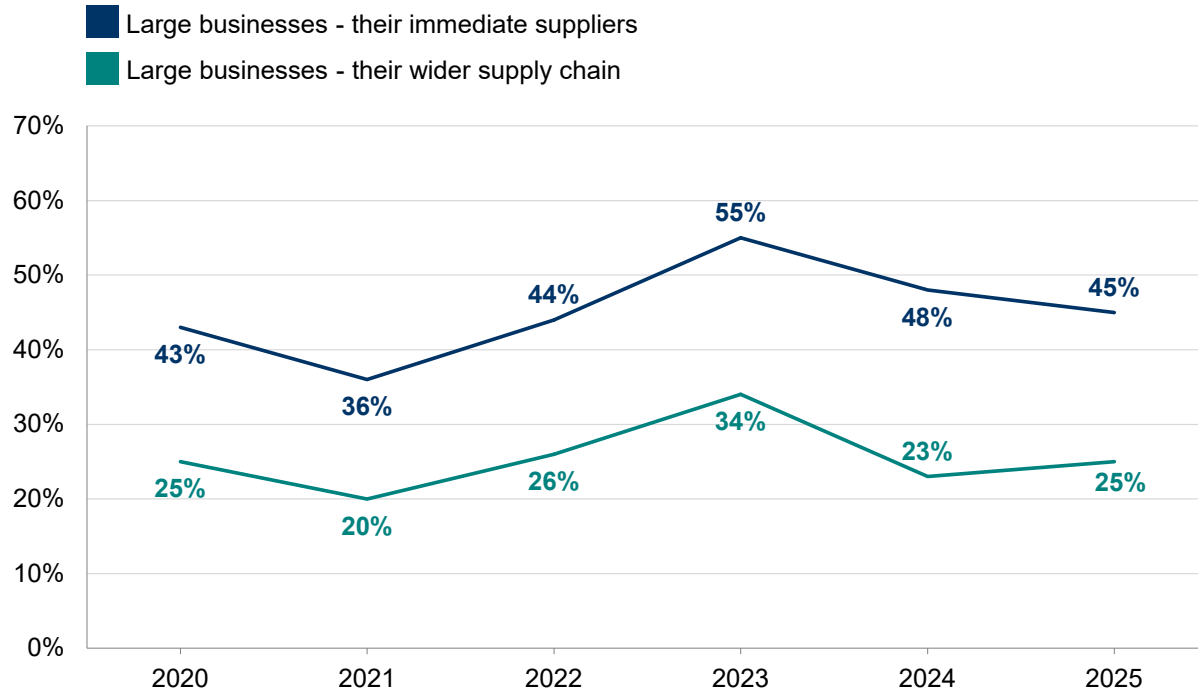
Business size	Their immediate suppliers	Their wider supply chain
Micro businesses	11%	6%
Small businesses	21%	11%
Medium businesses	32%	15%
Large businesses	45%	25%
Businesses overall	14%	7%
Charities overall	9%	4%

Bases: 2,180 all businesses; 1,014 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 1,081 charities

Trends over time

This question has been asked since the 2020 study and remains relatively stable at the overall level. As outlined in Figure 3.3, there was an increase among large businesses saying they reviewed the risks posed by their immediate suppliers (55%) and wider supply chain (34%) in 2023, this fell back down to pre-2023 levels in 2024 (48% reviewing risks posed by immediate suppliers and 23% reviewing the wider supply chain) and continued to remain in line this year (45% reviewing risks of immediate suppliers and 25% reviewing risks of the wider supply chain).

Figure 3.3: Percentage of organisations 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.

Weighting approach was changed in 2020 and sample frame was changed in 2023, changes are outlined in the separately published Technical Annex, both changes are expected to have a negligible impact on comparability across years.

Cyber security considerations when purchasing software
A new question for 2025 adds to the theme of managing risk, by asking about the role that cyber security considerations played when purchasing new software. As shown in Figure 3.4, around a fifth of businesses (21%) and charities (22%) considered cyber security to a large extent when purchasing software. For the bulk of businesses and charities however, it was not a major concern (37% of businesses and 29% of charities) and for sizeable minority (14% of businesses and 16% 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 (72%), whereas micro businesses were more likely to not consider it at all (16%).

Figure 3.4: Role of cyber security considerations when purchasing new software

We consider cyber security when purchasing new software to…

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 -
Businesses	21	19	37	14
Charities	22	15	29	16

Bases: 2,180 businesses; 1,081 charities

Qualitative insights on broad supply chain risks
Knowledge or understanding of supply chain risk continued to be a challenge for businesses and charities. Some organisations reported reviewing their suppliers' cyber security arrangements only after experiencing 'near misses', while others assume that larger suppliers possess stronger cyber security practices and therefore did not need oversight.

> "The big guys will be fine, but, you know, some of these, they get the people who do companies that do galvanizing, you know, that they're quite small and fairly basic." **Managing director, Medium business**

Larger businesses typically expressed greater concern about cyber risk from suppliers than smaller businesses or charities. It was evident among smaller businesses that there was limited knowledge and awareness of the full extent of their supply chains. For example, this could include suppliers of website services, social media platforms, and other digital services.

> "I don't think others fully appreciate the whole chain. It's not just customers, it's suppliers it's all interactions, it's all communication. It could be social media, it could be websites." **General manager, Small business**

Businesses and charities often placed significant trust in their suppliers, potentially creating cyber vulnerabilities and weaknesses. Some smaller businesses reported relying on third-party IT providers to determine whether they pursued specific accreditations, such as Cyber Essentials. Not all IT partners informed businesses or charities about the potential benefits of gaining these accreditations.

Participants' approaches to assessing software risk also differed. Some thoroughly vetted software for potential risks, while others did not.

> “I think as long as it’s got options of two factor authentication and single sign on, that would be ideal criteria. But sometimes it’s more what fits for purpose, sadly.” **IT manager, Medium business**

Where software was assessed for cyber security considerations, vetting processes differed depending on the nature of the data the software would be using. Some larger businesses stated that low-cost software not involving sensitive data would typically bypass IT checks, while others maintained that all software must undergo due diligence.

Qualitative insights on Digital Service Providers (DSPs)
The qualitative interviews also looked at perceptions of the risks posed by Digital Service Providers (DSPs), such as cloud service providers. Among the interviewees that discussed the topic, this covered a wide range of DSPs, including general IT service providers (including hardware and software maintenance), cloud storage providers, network monitoring, threat identification, and training providers.

Organisations tended to have a broad understanding of who their DSPs were and their reliance on them for IT and cyber security needs. However, when asked about reasons for choosing a certain supplier it was rare that cyber security had been a driving factor in the choice of provider, and in a number of cases it had not been a consideration at all.

Whilst cyber security was not commonly raised as a consideration when choosing a DSP, the focus centred more on an existing relationship, a good reputation or track record and financial cost. There was some acknowledgement of the potential cyber risks posed by using DSPs, but organisations tended to maintain their confidence in them, particularly with large DSPs.

> “Yes, because they’re all multinational organisations. I wouldn’t imagine they would be multinational organisations with poor cyber.” **CEO, Small business**

> “I’ve never given it a great deal of thought, but I assume the people that I spend the most money with will be the larger companies who I assume will have that in place, although I’ve never investigated that.” **Proprietor, Micro business**

> “I would imagine it wouldn’t be a Customer Relationship Management system if it didn’t have really good cyber security… that’s an

> assumption… never asked them." **CEO, Small business**

Smaller businesses and charities emphasised the vital role of their DSPs, while larger businesses typically used DSPs for niche security tasks.

> "They have control of all of our servers. So any breach that they have would be potentially a breach for us as well. I guess we just have faith that they're the professionals." **Head of operations, Small business**

A key theme that emerged throughout the qualitative interviews was the prevalence of longstanding contracts with DSPs. Some of these contracts predated the current IT contact's tenure at the company. Regular tendering or reassessment of DSPs appeared rare. This suggested that businesses and charities may be averse to change regarding cyber security practices, or it may highlight a reactive rather than proactive approach to cyber risk management.

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 (70%) had one in place. As shown in Figure 3.5, 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 (58% medium and 66% large). However, the proportion of high-income charities that had a strategy in place has fallen from roughly half (47%) in 2024 to around four in ten (39%) this year.

Figure 3.5: Percentage of organisations that have a formal cyber security strategy in place

Organisation type	
Medium businesses	57%
Large businesses	70%
High-income charities	39%

Bases: 413 medium businesses; 188 large businesses; 343 high-income charities

Among the larger organisations that had a cyber security strategy in place, around eight in ten businesses (82%) and three-quarters of charities (76%) 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 (45%) and a third of charities (34%) reported being insured against cyber security risks in some way. In most cases, as Figure 3.6 shows, organisations' cyber security insurance was part of a wider insurance policy: only 7% of businesses and 5% of charities had a specific cyber security insurance policy. Larger businesses (18% of medium businesses and 27% of large businesses) and high-income charities (23%) were more likely to have a specific policy in place.

As in previous years, small and medium businesses were more likely than businesses overall (45%) to have some form of cyber insurance (62% small businesses and 65% 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 (20%) and charities (19%) 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 3.6: Percentage of organisations that have the following types of insurance against cyber security risks

Organisation	Cyber security cover as part of a wider insurance policy	A specific cyber security insurance policy
Micro businesses	36%	5%
Small businesses	45%	17%

Organisation	Cyber security cover as part of a wider insurance policy	A specific cyber security insurance policy
Medium businesses	47%	18%
Large businesses	26%	27%
Businesses overall	38%	7%
Charities overall	29%	5%

Bases: Split-sample half A: 491 micro businesses; 269 small businesses; 189 medium businesses; 97 large businesses; 1,046 businesses overall; 558 charities overall

Trends over time
Compared to the 2024 survey, the proportion of businesses with some form of insurance has remained broadly consistent (43% in 2024 and 45% in 2025), reflecting that stability has been recovered since a dip in 2023 (37%). The increase since 2023 was largely driven by higher inclusion of cyber security cover as part of a wider insurance policy amongst micro businesses (up from 29% in 2023 to 36% in 2025) and small businesses (up from 33% in 2023 to 45% in 2025). More small businesses in 2025 had some form of cyber insurance (62%) compared to 2024 (49%).

The proportion of charities with some form of insurance has remained consistent (34% in both 2025 and 2024, and 33% in 2023).

The 2025 survey included a new question that asked organisations, who did not have any cyber insurance, why they did not have it. As shown in Figure 3.7, it not being a budgetary priority (34% of businesses and 41% of charities) and lack of awareness of cyber insurance (37% of businesses and 31% of charities) were the two largest barriers to holding a cyber insurance policy.

Figure 3.7: Reasons why organisations are not covered by a cyber insurance policy

Reason	Businesses	Charities
Not a budgetary priority	34%	41%

Reason	Businesses	Charities
Not aware of cyber insurance	37%	31%
Leadership not interested in cyber insurance	28%	18%
Too expensive	13%	13%
Coverage not broad enough	5%	2%
Don’t know	11%	20%

Bases: Those that don’t have a cyber insurance policy: 273 businesses; 213 charities

Qualitative insights on cyber insurance
Cost-benefit analysis of cyber insurance emerged as a key theme through the qualitative interviews. Businesses and charities that held cyber insurance rarely made claims, even when eligible. Organisations typically felt that claims were not considered worthwhile overall, primarily due to an unfavourable cost-benefit analysis. This was especially apparent when discussing the potential increase in future premiums after making a claim. It was asserted by larger businesses that investing in cyber controls and recovery was more beneficial than investing in insurance itself.

> “The scale of the incidents we had never got to the point where it was going to be worthwhile. The increase in premiums and the excess etc., it just wasn’t going to be economical to make a claim.” **Head of cyber security, Large business**

There was also a lack of knowledge around cyber insurance, with organisations often unaware of cyber insurance as a separate product from general insurance policies. However, where organisations were aware of, or had cyber insurance, some reported that their insurance providers offered valuable advice and encouragement to improve their cyber security practices. This suggests that cyber insurance may provide benefits beyond financial coverage, such as expert guidance and increased accountability.

> “It was felt that particularly given our relatively limited budget, that it was better actually having the insurance to mobilise resources in the event of [a breach], rather than having the budget to be more preventative. Felt like it was a relatively good use of resources to invest in kind of ready to go, reactive measures. We’ve not had to make any formal claims, but

> we do engage with them with near misses and breaches that won't require a claim." **Director of Digital, Charity**

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 3.8. 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, passwords, network firewalls, cloud backups and restricted admin rights each administered by at least two-thirds of businesses. The least common rules and controls were two-factor authentication (2FA), separated Wi-Fi networks, applying software updates, use of Virtual Private Networks (VPNs), and user monitoring (with exact percentages included in Figure 3.8).

Figure 3.8: Percentage of organisations that have the following rules or controls in place

Rules or controls	Businesses	Charities
Up-to-date malware protection	77%	64%
A password policy that ensures that users set strong passwords	73%	57%
Firewalls that cover the entire IT network, as well as individual devices	72%	49%
Backing up data securely via a cloud service	71%	58%
Restricting IT admin and access rights to specific users	68%	68%
Only allowing access via organisation-owned devices	61%	34%

Rules or controls	Businesses	Charities
Security controls on organisation-owned devices (e.g. laptops)	58%	43%
An agreed process for staff to follow with fraudulent emails or websites	55%	39%
Backing up data securely via other means	47%	39%
Rules for storing and moving personal data securely	45%	50%
Any Two-Factor Authentication (2FA) for networks/applications	40%	35%
Separate Wi-Fi networks for staff and visitors	33%	27%
A policy to apply software security updates within 14 days	32%	21%
A virtual private network, or VPN, for staff connecting remotely	31%	20%
Monitoring of user activity	30%	31%

Bases: 2,180 businesses, 1,081 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 (98%)
- restricting admin rights (97%)
- data backups, either via the cloud or other means (96%)
- security controls on their devices (95%)
- up-to-date malware protection (94%)
- network firewalls (94%)
- separate Wi-Fi for staff and visitors (93%)
- requirements for two-factor authentication (92%).

Trends over time
Compared to 2024, the deployment of controls and procedures has remained stable for several procedures, but has fallen slightly for some

controls among businesses:

- using up-to-date malware protection (down from 83% in 2024 to 77% in 2025)
- restricting admin rights (down from 73% in 2024 to 68% in 2025)
- backing up data securely via means other than a cloud service (down from 55% in 2024 to 47% in 2025).

In 2024, the survey saw several rules or controls (up-to-date malware protection, restricting admin rights, network firewalls and agreed processes for phishing attacks) increase upon a previous trend of decline, but 2025 results suggest the upward trajectory has not been sustained.

It is important to note that this decline on some measures in 2025 mainly reflect shifts from 2024 in micro businesses and, to a lesser extent, small and medium businesses. On each of the technical controls in Figure 3.8, large businesses remain in line with where they were in 2024.

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

3.5 Staff training and awareness raising

This survey does not explore cyber security skills and training in detail, given that there is 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.

Our results (Figure 3.9) show that in the last 12 months, around a fifth of businesses (19%) and charities (21%) have provided some form of staff training. Over half of all medium businesses (54%), three-quarters of large businesses (76%) and around half of high-income charities (47%) provided training.

Figure 3.9: Percentage of organisations that have had training or awareness raising sessions on cyber security in the last 12 months

Organisation type	
Micro businesses	15%
Small businesses	34%
Medium businesses	54%
Large businesses	76%
Businesses overall	19%
Charities overall	21%

Bases: 1,014 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,180 businesses overall; 1,081 charities overall

Trends over time
Since the 2021 survey, the proportion of large businesses running training has consistently increased. For example, it was 47% for large businesses in 2021, compared to 61% in 2022, 77% in 2023, and 80% in 2024. In 2025 the proportion looks to have plateaued (76%).

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 (21%), Chief Executive (16%), or another senior management role (13%). Very

few micro businesses had someone specifically in an IT-role looking after cyber security matters (1%)

- 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 (25%), those with another (unspecified) senior management role (18%) or Chief Executives (15%)
- in four in ten large businesses, it was either the IT director (19%) or an IT manager, technician or administrator (20%) looking after cyber security. The respective figures for medium sized businesses were 12% and 11%
- in three in ten charities (29%), 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 (17%), general or office managers (15%), Chief Executives (13%), or IT Directors (10%).

3.7 Outsourcing of cyber security functions

Almost half of businesses (44%) and around a quarter of charities (27%) 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 3.10 shows, outsourcing of cyber security was substantially higher among small (62%) and medium (68%) businesses, as opposed to micro (39%) and large (50%) businesses. This pattern has also been evidenced in previous years. It is possible that large businesses were relying more on internal cyber security expertise than on outsourcing, while micro, small and medium businesses perhaps could not afford to recruit specialists to the same extent. This year, the proportion of small businesses likely to have an external cyber security provider was significantly higher than in 2024 (56% in 2024 and 62% in 2025).

Figure 3.10: Percentage of organisations that have an external cyber security provider

Organisation type	
Micro businesses	39%
Small businesses	62%
Medium businesses	68%
Large businesses	50%

Organisation type	
Businesses overall	44%
Charities overall	27%

Bases: 1,014 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,180 businesses overall; 1,081 charities overall

3.8 Cyber security policies and other documentation

Do organisations formally document their approaches?
A third of businesses (36%) and charities (35%) 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 (32%), and a smaller proportion of charities (23%) had a business continuity plan that covered cyber security.

Figure 3.11 shows strong differences by size, with the majority of medium and large businesses having each form of documentation. Similarly to having an external cyber security provider, small businesses have seen significant increases in both having a formal policy covering cyber security risks (up from 51% in 2024 to 59% in 2025) and having a business continuity plan that covered cyber security (up from 44% in 2024 to 53% in 2025).

Figure 3.11: Percentage of organisations that have a cyber security policy or business continuity plan

Organisation type	A formal policy or policies covering cyber security risks	A business continuity plan that covers cyber security
Micro businesses	30%	27%
Small businesses	59%	53%
Medium businesses	74%	70%

Organisation type	A formal policy or policies covering cyber security risks	A business continuity plan that covers cyber security
Large businesses	87%	79%
Businesses overall	36%	32%
Charities overall	35%	23%

Bases: 1,014 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,180 businesses overall; 1,081 charities overall

When were policies last reviewed?
Of businesses and charities that had cyber security policies in place, the majority reviewed them at least annually (79% businesses and 70% charities). However, as detailed in Figure 3.12, this did leave one in five charities who reviewed their cyber security policies less than annually (21%).

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

Figure 3.12: When organisations last created, updated, or reviewed their cyber security policies or documentation

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	24	23	32	10	3	8
Charities	19	16	35	12	9	9

Bases: Those with cyber security policies in place: 1,140 businesses; 491 charities

What is covered in cyber security policies?

As Figure 3.13 indicates, cyber security policies tend to cover a range of topics. The aspects most often covered were data storage (81% businesses and 85% charities) and the appropriate use of the organisation's IT devices (81% businesses and 75% charities).

Figure 3.13: Percentage of organisations with cyber security policies that have the following features in their cyber security policies

Features	Businesses	Charities
How data is supposed to be stored	81%	85%
What staff are permitted to do on organisation's IT devices	81%	75%
Use of cloud computing	66%	62%
Remote or mobile working	64%	64%
Use of network-connected devices	63%	57%
What can be stored on removable devices (e.g. USB sticks)	61%	59%
Digital Service Providers such as cloud services	57%	48%
Use of personally-owned devices for business activities	54%	59%

Bases: Those with cyber security policies in place: 1,140 businesses; 491 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 awareness of Cyber Essentials among businesses (12%) and charities (15%). Despite this lack of awareness, a slightly higher proportion of businesses and charities did have technical controls in these five areas.

The survey asked questions which corresponded to the five areas[footnote 10]. In total, 21% of businesses and 12% of charities reported having technical controls in all five areas. As might be expected, this was considerably higher for medium businesses (47%), large businesses (59%) and high-income charities (33%).

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

We also asked organisations if they recalled adhering to either the Cyber Essentials or Cyber Essentials Plus standards. Both required 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 3% of businesses and charities reported adhering to Cyber Essentials, which matches 2024 figures (both 3%). Just 1% of businesses and charities said they adhered to the Cyber Essentials Plus standard. Among large businesses, this rose to 21% holding Cyber Essentials and 10% achieving Cyber Essentials Plus. This continues 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. A quarter of businesses (25%) and around one in six charities (16%) did not know if their organisation adheres 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

The qualitative interviews touched on the rationale for organisations seeking accreditation, among organisations that had done so. Across interviews, organisations primarily spoke about Cyber Essentials and to a lesser extent about ISO 27001.

There seemed to be a growing awareness of accreditations such as Cyber Essentials and ISO 27001 and on the whole, they were viewed positively. The overall reasons for seeking accreditation reflected themes that had been raised in previous years of this study, including demand from clients, pressure from board members and for peace of mind for stakeholders. Medium and larger businesses were particularly likely to state that client requirements determined their likelihood of becoming accredited.

> "It's only a matter of time before [client name] demand that." **General manager, Small business**

The primary barriers to achieving these cyber accreditations were typically cost and concerns about value for money, as well as the perceived difficulty of the accreditation process.

> "I am looking at whether it's cost effective for me to go for Cyber Essentials." **Business owner, Micro business**

Some businesses mentioned they preferred ISO27001 as an accreditation than Cyber Essentials, as it seemed more robust. This demonstrated the varied perception of different accreditations amongst businesses.

Where charities possessed or were working towards an accreditation, this tended to be Cyber Essentials, rather than Cyber Essentials Plus. Again, this may be due to a lack of resource often cited by charities.

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 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 2023, the 2025 results for the 10 Steps to Cyber Security are only comparable to 2023 and 2024.

The 10 Steps are actions that all organisations can take, but the guidance is 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. Any significant changes from last year have been noted in the table by providing the 2024 figure.

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

Step description	Businesses	Medium businesses	Large businesses	Charities
1 **Risk management -** organisations have undertaken a cyber security risk assessment	29%	57%	70%	29%
2 **Engagement and training -** organisations have carried out staff training or awareness raising activities	19%	54%	76%	21%
3 **Asset management -** organisations have a list of critical assets	29%	57%	76% (compared with 65% in 2024)	30%
4 **Architecture and configuration -** organisations have at least three of the following technical rules or controls: up-to-date malware	75% (compared with 81% in 2024)	95% (compared with 98% 2024)	100%	60%

Step description	Businesses	Medium businesses	Large businesses	Charities
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 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	32%	53%	64%	21%
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	40%	74%	92%	35%
7 **Data security -** organisations have cloud backups or	83% (compared with 88% in 2024)	94%	96%	73%

Step description	Businesses	Medium businesses	Large businesses	Charities
other kinds of backups				
8 **Logging and monitoring -** organisations fulfil at least one of the following criteria: using specific tools designed for security monitoring, such as Intrusion Detection Systems, or doing any monitoring of user activity	45%	80%	90%	41%
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	30%	61%	85%	28%
10 **Supply chain security -** organisations monitor risks from	15%	35%	48%	10%

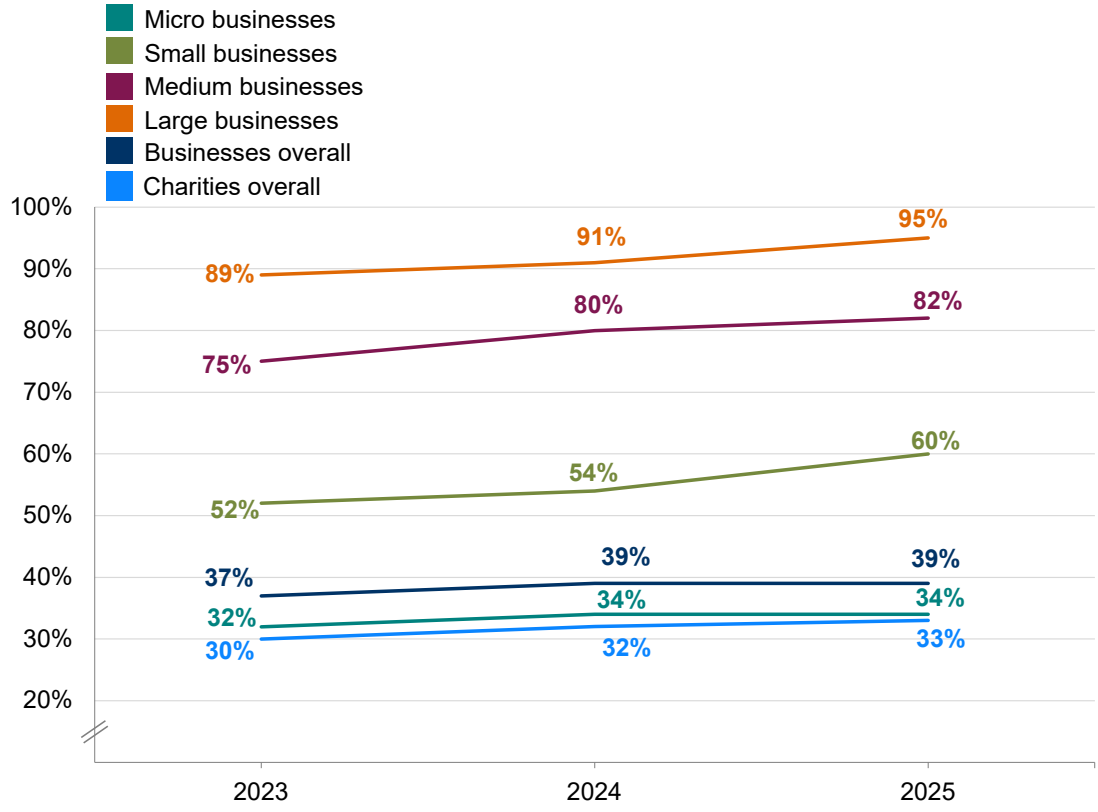
Step description	Businesses	Medium businesses	Large businesses	Charities
suppliers or their wider supply chain				

The majority of businesses (89%) and charities (82%) had undertaken key actions associated with at least one of the 10 Steps. The proportion of charities doing so remained in line with 2024 (82%), however, the proportion of businesses was lower than in 2024 (94%).

Two-fifths of businesses (40%) and a third of charities (33%) had taken action on 5 or more of the 10 Steps in 2025, as Figure 3.14 shows. This was also much higher in large businesses, where 100% 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 (12%) and large (22%) businesses.

Figure 3.14: 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

While results have remained consistent for businesses and charities at the overall level, large businesses have seen a significant increase in the proportion undertaking action in 5 or more of the 10 Steps (100% compared to 91% in 2024) (Figure 3.14).

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 11], 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 three in ten charities (30%) reported having experienced 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 61,000 charities having identified a cyber breach or attack in the last 12 months.

- Overall prevalence of experiencing any cyber breach or attack has declined this year among businesses compared to 2024 (50%), driven by a decrease in micro (41% down from 47% in 2024) and small (50% down from 58% in 2024) businesses identifying a cyber breach or attack.
- Prevalence of breaches and attacks among large businesses (74%, the same as in 2024) and medium businesses (67% in line with 70% in 2024) has remained consistent.
- There has been a decline in the proportion of businesses reporting phishing attacks (from 42% in 2024 to 37% in 2025), driven by decreases among micro (from 40% in 2024 to 35% in 2025) and small (49% in 2024 to 42% in 2025) businesses.
- Phishing attacks remained the most prevalent type of breach or attack by far (experienced by 85% of businesses and 86% of charities that experienced a breach or attack in the last 12 months), and continue to be ascribed as the most disruptive type of breach or attack (65% of businesses and 63% of charities that experienced a breach of attack).
- While the proportion of organisations experiencing a negative outcome from a breach remained consistent with 2024, (16% of businesses and 16% of charities in 2025 compared to 13% of businesses and 12% of charities in 2024), specific outcomes show shifts. To note, the differences in these percentages were not statistically significant. Businesses have experienced a significant increase in temporary loss of access to files or networks as a specific outcome (7%, up from 4% in 2024) and charities have seen a significant increase in loss of access to a third-party service (5%, up from 1% in 2024) .
- The average self-reported mean cost of the most disruptive breach or attack among businesses in the last 12 months was £1,600 including those giving a £0 response (and £3,550 excluding £0 responses). For charities in the last 12 months it was £3,240 including £0 responses (and £8,690 excluding £0 responses).

4.1 Note on comparability to previous year

In the 2024 survey some significant wording changes were made to the question that sought to capture overall incidence of breaches and attacks (Q53A). This meant that last year no direct comparisons could be made between 2024 and previous years of the survey.

This year no changes were made to the wording of Q53A, which means that results can be compared with 2024 (but not to prior years).

4.2 Identified breaches or attacks

Just over four in ten businesses (43%) and three in ten charities (30%) reported having experienced any kind of cyber security breach or attack in the last 12 months[footnote 12]. This accounts for approximately 612,000 businesses and 61,000 registered charities although these estimates, like all survey results, are subject to a margin of error (see Appendix A).

Prevalence of cyber security breaches or attacks amongst businesses has seen a decline from 2024, down from 50% in 2024 to 43%. This was largely driven by a decline in phishing attacks among micro (from 40% in 2024 to 35% in 2025) and small (49% in 2024 to 42% in 2025) businesses.

As shown in Figure 4.1 [footnote 13], medium (67%) and large (74%) businesses were more likely to have experienced a cyber breach or attack in the last 12 months compared to micro businesses (41%) and small businesses (50%). 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.

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

Organisation type	2025	2024
Micro businesses	41%	47%
Small businesses	50%	58%
Medium businesses	67%	70%
Large businesses	74%	74%
Businesses overall	43%	50%

Bases 2025: 1,013 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,179* businesses overall. Bases 2024: 1,060 micro businesses; 506 small businesses; 264 medium businesses; 170 large businesses; 2,000 businesses overall

Trends over time

The prevalence of cyber security breaches or attacks amongst businesses has seen a decline from 2024, down from 50% in 2024 to 43% (Figure 4.1).

The decline was driven by significant decreases among micro and small businesses (micro businesses now 41%, down from 47% in 2024 and small businesses now 50% down from 58% in 2024). The prevalence of cyber security breaches or attacks has remained stable for medium and large businesses compared to 2024.

Looking at prevalence of cyber breaches or attacks by sector (Figure 4.2), businesses in the information or communication sector (69%) and the professional, science or technical sector (55%) 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 (30%) and the retail or wholesale sector (32%).

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

Industry sector	
Information or communications	69%
Professional, scientific or technical	55%
Administration or real estate	48%
Finance or insurance	48%
Utilities or production	48%
Entertainment or service	42%
Health or social care	41%
Construction	40%
Transport or storage	35%
Retail or wholesale	32%
Food or hospitality	30%
Businesses overall	43%

Bases: 130 information or communications businesses; 273 professional, scientific or technical businesses; 320 administration or real estate businesses; 141 finance or insurance businesses; 150 health or social care businesses; 231 construction businesses; 94 transport or storage businesses; 357 retail or wholesale businesses; 168 food or hospitality businesses; 2,179 businesses overall

By business sector, there has been a decrease in cyber breaches and attacks identified within the administration or real estate sector (48% compared to 59% in 2024), the wholesale or retail sector (32% compared to 43% in 2024) and the utilities or production sector (48% compared to 62% in 2024). It is worth noting that this was not simply a reflection of having more micro and small size businesses within these sectors as the proportion of businesses in these size bands is in line with businesses overall.

In addition, businesses based in London were more likely than businesses overall to experience a breach or attack (51% compared to 43% overall). 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 (42%) and high-income charities (64%) were significantly more likely to have identified a breach or attack compared to low-income charities (24%) and to charities overall (30%).

Trends over time

Prevalence of cyber security breaches or attacks amongst charities (Figure 4.3) has remained in line with 2024 (32% in 2024 and 30% in 2025). There has also been no significant change in prevalence of attacks or breaches by charity size.

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

Charity type	2025	2024
Low-income charities	24%	25%
Medium-income charities	42%	49%
High-income charities	64%	66%
Charities overall	30%	32%

Bases: 2025: 446 low-income charities, 292 medium-income charities, 343 high-income charities; 1,081 charities overall. Bases: 2024: 464 low-income

charities, 205 medium-income charities, 335 high-income charities; 1,004 charities overall

Types of breaches or attacks identified

Figure 4.4 shows the types of breaches and attacks that organisations report having, among those that have identified any in the last 12 months. The most common by far was phishing (85% among affected businesses and 86% among affected charities) defined in the context of this survey as staff receiving fraudulent emails or being directed to fraudulent websites. This equated to 37% of all businesses and 26% of all charities experiencing phishing breaches or attacks.

Phishing attacks were followed, to a much lesser extent, by people impersonating organisations in emails or online (34% businesses and 35% charities who identified an attack equated to 15% of all businesses and 11% of all charities) and then viruses or other malware (18% businesses and 14% charities who identified an attack, equated to 8% of all businesses and 4% of all charities).

Figure 4.4: Percentage of types of breaches or attacks in the last 12 months, among the organisations that have identified any breaches or attacks

Type	Businesses	Charities
Phishing attacks, i.e. staff receiving fraudulent emails or arriving at fraudulent websites	85%	86%
Others impersonating, in emails or online, your organisation or your staff	34%	35%
Organisation’s devices being targeted with other malware (e.g. viruses or spyware)	18%	14%
Takeovers or attempts to take over your website social media accounts or email accounts	7%	9%
Organisation’s devices being targeted with ransomware	6%	4%
Hacking or attempted hacking of online bank accounts	6%	5%
Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or services	5%	4%

Type	Businesses	Charities
Unauthorised accessing of files or networks by staff even if accidental	2%	4%
Unauthorised accessing of files or networks by people outside your organisation (other than staff or students)	2%	3%
Unauthorised listening into video conferences or instant messaging*	0%	0%
Any other breaches or attacks	4%	4%

Bases: Those that identified a breach or attack in the last 12 months: 1,132 businesses, 445 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%”.

Among the organisations identifying any breaches or attacks, just under half (45% of these businesses and 46% of these charities) said they had only experienced phishing attacks and no other kinds of breaches or attacks. The proportion only experiencing phishing attacks was lower among large (15%) and medium (26%) businesses.

Among businesses identifying any breaches or attacks, large, and to some extent medium businesses, were most likely to report a range of cyber breaches and attacks, including:

- phishing attacks (94% of large businesses compared with 85% businesses overall)
- impersonation (72% of large businesses and 64% of medium businesses, compared with 34% businesses overall)
- malware (36% of large businesses, compared with 18% businesses overall)
- denial of service attacks (15% of large businesses, compared with 5% businesses overall)
- ransomware (14% of large businesses compared with 6% businesses overall)
- takeovers (12% of large businesses compared with 7% businesses overall)
- unauthorised access by people within the organisation (12% of large businesses and 7% of medium businesses, compared with 2%

businesses overall)

- unauthorised access by people outside the organisation (8% of large businesses and 5% of medium businesses, compared with 2% businesses overall)
- unauthorised listening into video conferences or instant messaging (4% large businesses and 1% medium businesses versus less than 0.5% businesses overall)

Small businesses that experienced a breach or attack were more likely than businesses overall to identify:

- hacking or attempted hacking of online bank accounts (9% small businesses compared with 6% businesses overall)
- impersonation (51% small businesses compared with 34% businesses overall)

Among charities identifying any breaches or attacks, high-income charities were more likely to report:

- people impersonating, in emails or online, the organisation or staff (61% compared with 35% charities overall)
- malware (17% compared with 14% charities overall)
- hacking or attempted hacking of online bank accounts (7% compared with 5% charities overall)
- denial of service attacks (5% compared with 4% charities overall)
- unauthorised access by people within the organisation (6% compared with 4% charities overall)

Whereas Figure 4.4 looked at the types of breaches or attacks of those that identified one in the last 12 months, looking at the types of breaches or attacks as a proportion of all organisations shows that 37% of businesses overall and 26% of charities overall experienced a phishing attack and 15% of businesses overall and 11% of charities overall experienced impersonation. The third most common breach or attack - devices being targets with malware, viruses or spyware – was experienced by 8% of businesses overall and 8% of charities overall.

When looking at the proportion of all organisations that have experienced different types of breaches or attack in the last 12 months compared to 2024, there have been a couple of significant shifts. There has been a significant decline in the proportion of businesses reporting phishing attacks (from 42% in 2024 to 37% in 2025), driven by decreases among micro (from 40% in 2024 to 35% in 2025) and small (49% in 2024 to 42% in 2025) businesses. There has also been a significant increase in the proportion

reporting other breaches or attacks (that is any other breach or attack that is not listed in figure 4.4), from 1% in 2024 to 2% in 2025.

4.3 Frequency of breaches or attacks

Among those identifying any breach or attack in the previous 12 months, as shown in Figure 4.5, around half of businesses (52%) said they experienced a breach or attack at least once a month, and one in three said it happened at least once a week (29%). For charities, around two in five (39%) said they experienced a breach or attack at least on a monthly basis, and for one in five this was at least once a week (18%). There were no significant changes by business size in the frequency of breaches or attacks. For both businesses and charities this remains in line with 2024.

Figure 4.5: How often organisations have experienced breaches or attacks in the last 12 months

Organisation type	% Only Once	% Less than once a month	% Once a month	% Weekly or more frequently -
Businesses	19	28	23	29
Charities	22	35	21	18

Bases: Those that identified a breach or attack in the last 12 months: 1,132 businesses, 445 charities

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 65% of the businesses and 63% of the charities). Figure 4.6 also shows that people impersonating organisations or staff was the attack next most commonly reported to be disruptive.

Figure 4.6: Percentage that report the following types of breaches or attacks as the most disruptive, across all who experienced a breach in the last 12 months

Type	Businesses	Charities
Phishing attacks, i.e. staff receiving fraudulent emails or arriving at fraudulent websites	65%	63%
People impersonating, in emails or online, your organisation or your staff	18%	20%
Takeovers or attempts to take over your website, social media accounts or email accounts	4%	6%
Hacking or attempted hacking of online bank accounts	3%	4%
Your organisation’s devices being targeted with other malware (e.g viruses or spyware)	3%	3%
Your organisation’s devices being targeted with ransomware	3%	1%
Denial of service attacks, i.e. attacks that try to slow or take down your website, applications or online services*	3%	0%

Bases: Those that were able to specify a breach or attack experienced in the last 12 months: 1,032 businesses, 429 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 (68%) were significantly more likely than small (57%), medium (52%) and large (43%) businesses to have identified phishing as the most disruptive breach. Whereas large (30%), medium (32%) and small (28%) businesses were significantly more likely to have stated impersonation as the most disruptive breach compared to micro businesses (15%).

Diagnosing why phishing attacks were the most disruptive breach or attack

New for 2025, those that experienced more than one type of breach or attack and then selected phishing as the most disruptive type of attack were asked a follow up question about why phishing was the most disruptive. The most common reason given was that they resulted in people impersonating the organisation or staff in emails or online (19% of businesses and 25% of charities). This was followed, to a lesser extent, by breaches or attacks being reported as disruptive because they led to being targeted with

malware (9% for both businesses and charities) or ransomware (7% of businesses and 1% of charities), or resulted in hacking (9% for businesses and 2% for charities).

A sizeable minority (15% of businesses and 20% of charities) gave a response in the 'other specify' category where they were able to provide some verbatim comments about why they had found phishing to be the most disruptive. Reasons given centred on the time taken to deal with phishing incidents, both time from the staff having to report them and the time taken by the IT or management team to investigate the incidents to assess whether any follow up action was needed.

It is also worth noting that almost half of businesses (45%) and four in ten charities (40%) responded 'none of the above' when prompted with a range of outcomes that resulted from the phishing attack. This suggested it was possible there are a range of other reasons for phishing attacks being disruptive that have not currently been captured by the survey.

Qualitative interviews found similar reasons for phishing causing so much disruption to businesses and charities. Organisations in the 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.

> "It's just a lot of more daily vigilance on the potential scam" **Customs Specialist, Medium business**

In addition, time was being spent by organisations on training staff on how to recognise potential phishing attacks and how to report it if they suspected they had received anything. This was further compounded by a growing concern on the use of AI in phishing scams and the need to stay up to date with the latest practices in minimising the threat from them.

> 'I think it's going to get more and more difficult with what's out there with AI. I think there's more for us to do and protect the end user and educate them.' **IT manager, Medium business**

> "Phishing has been and will remain a key challenge which is tackled by a combination of technology, including obfuscating usernames from email addresses and use of AI to detect potential phishing methods." **Head of IT and systems, Charity**

Time taken to recover from the most disruptive breach or attack

When considering their most disruptive breach or attack, the vast majority of businesses (92%) and charities (89%) affected reported being able to restore their operations within 24 hours (Figure 4.7). Furthermore, almost eight in ten businesses (77%) and charities (78%) said it took ‘no time at all’ to recover.

Figure 4.7: How long it took to get operations back to normal after their most disruptive breach or attack was identified

Organisation type	% No time at all	% Less than a day	% More than a - day
Businesses	77	15	8
Charities	78	11	10

Bases: Those that were able to specify a breach or attack experienced in the last 12 months: 1,032 businesses, 429 charities

4.5 How organisations are affected?

Outcomes of breaches or attacks
Among the businesses and charities that experienced any breaches or attacks, around one in six (16%) also experienced a negative outcome as a result (listed in Figure 4.8). The low proportion stating a negative outcome indicates that a large proportion of attacks are unsuccessful. The temporary loss of access to files or networks and disruption to websites are the most commonly reported outcomes. However, as Figure 4.8 indicates, cyber breaches and attacks that overcome defences can have a wide range of outcomes.

Figure 4.8: Percentage that had any of the following outcomes, among the organisations that have identified breaches or attacks in the last 12 months

Type	Businesses	Charities
Any listed outcome	16%	16%
Temporary loss of access to files or networks	7%	5%
Web applications / online services were taken down or made slower	6%	6%

Type	Businesses	Charities
Software or systems were corrupted or damaged	3%	2%
Lost access to any third-party services you rely on	3%	5%
Personal data was altered, destroyed or taken	2%	1%
Money stolen	2%	2%
Physical devices or equipment were damaged or corrupted	2%	1%

Bases: Those that identified a breach or attack in the last 12 months: 1,132 businesses, 445 charities

Large (29%) and medium (20%) businesses were more likely than businesses overall to have experienced an outcome listed in Figure 4.8. Differences among large and medium businesses on individual outcomes include:

- 10% of large businesses temporarily lost access to files or networks compare with 7% businesses overall
- 7% of large businesses and 5% of medium businesses lost access to a third-party service they rely on compared with 3% businesses overall
- 5% of medium businesses had software or system damages compared with 3% businesses overall
- 5% of large businesses lost customers' personal data compared with 2% businesses overall
- 6% of large businesses had physical devices or equipment damaged compared with 2% businesses overall
- 4% of large businesses and 3% of medium businesses paid money in ransom compared with 1% businesses overall
- 5% of large businesses and 5% of medium businesses had their accounts or systems compromised for illicit purposes compared with 1% businesses overall

Trends over time

While the proportion of organisations experiencing a negative outcome from a breach remained consistent with 2024, (16% of businesses and 16% of charities in 2025 compared to 13% of businesses and 12% of charities in 2024), specific outcomes show shifts. To note, the differences in these percentages were not statistically significant. Businesses have experienced

a significant increase in temporary loss of access to files or networks as a specific outcome (7%, up from 4% in 2024). In addition, charities have seen a significant increase in loss of access to a third-party service as an outcome (5%, up from 1% in 2024).

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 4.9. Almost three in ten businesses (28%) and three in ten charities (30%) that have had any breaches or attacks reported being impacted in at least one of the ways noted in Figure 4.9.

Most commonly, breaches or attacks led to organisations having to take up new measures to prevent or protect against future cases (18% businesses and 15% charities) or having to employ additional staff time to deal with the breach or attack (17% businesses and 19% charities).

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

Type	2024	2025
Any Listed Impact	28%	30%
New measures needed to protect against future breaches or attacks	18%	15%
Additional staff time to deal with breach or attack or to inform customers or stakeholders	17%	19%
Stopped staff from carrying out their day-to-day work	9%	11%
Other repair or recovery costs	4%	3%
Prevented provision of goods or services to customers	3%	4%
Complaints from customers	2%	2%
Loss of revenue or share value	2%	4%
Discouraged you from carrying out a future business activity	2%	1%
Reputational damage	1%	1%
Goodwill compensation or discounts given to customers	1%	2%

Type	2024	2025
Fines from regulators or authorities or associated legal costs	0%	1%

Bases: Those that identified a breach or attack in the last 12 months: 1,132 businesses, 445 charities

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

- 32% needed extra staff time to deal with breaches or attacks (compared with 17% of all businesses identifying breaches or attacks)
- 26% of large businesses said they had to take up new measures to prevent or protect against future breaches or attacks (compared with 18% all businesses identifying breaches or attacks)
- 19% reported staff being stopped from carrying out their day-to-day work (compared with 9% all businesses identifying breaches or attacks)
- 8% reported the breach or attack prevented provision of goods or services to customers (compared with 3% all businesses identifying breaches or attacks).
- 6% reported receiving complaints from customers (compared with 2% all businesses identifying breaches or attacks).

A similar trend was observed for high-income charities. Whereas 30% of all charities identifying breaches or attacks reported an impact, this rose to 36% of high-income charities. In terms of individual impacts:

- 26% of high-income charities 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)
- 23% needed extra staff time to deal with breaches or attacks (compared to 19% 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 2024, and the proportion of businesses reporting an outcome remained consistent (13% in 2025 and 16% in 2025).

The proportion of businesses experiencing any impact following a cyber breach or attack also remained in line with last year for businesses overall (24% in 2024 and 28% in 2025). However, looking at individual impacts, there has been an increase among large businesses reporting that the breach or attack prevented provision of goods or services to customers (3% in 2024 to 8% in 2025).

The proportion of charities reporting an outcome following a cyber breach or attack (16%) remained consistent with 2024 (12%). However, among charities there has been a decline in those experiencing any of the impacts (30%, down from 41% in 2024). This decrease was seen most clearly across the medium-income and high-income charities, with 27% of mid-income charities reporting an impact (compared to 43% in 2024), and 36% of high-income charities reporting an impact (compared to 49% in 2024).

4.5 Financial cost of breaches or attacks

Each year, this survey series has attempted to capture the cost of cyber security breaches or attacks on organisations. The costs reported here are self-reported estimates, which may represent an underestimation of full financial impact.

As in previous years of the survey, we asked granular 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. Tables 4.1 to 4.4 show these self-reported cost estimates. Table 4.5 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 the a tables), as well as those with an actual outcome (shown in the b tables), such as a loss of assets or data. The latter subgroup of organisations tends to face higher costs, as these tables show.

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

To note, the way these cost estimates are compiled was substantially changed in the 2021 survey, so they cannot be compared to results from before 2021.

As displayed in Table 4.1, we cover the short-term direct costs of the most disruptive breach or attack. In the survey, we defined these as being any external payments that were made when the breach or attack was being dealt with. This includes, as examples offered to respondents:

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

Table 4.1a: Average short-term direct cost of most disruptive breach or attack from the last 12 months[footnote 14]

Across organisations identifying any breaches or attacks	All businesses	Micro/small businesses	Medium/large businesses	All charities
Mean cost	£530	£510	£990	£2,670
Median cost	£0	£0	£0	£0
Base	978	638	340	422

Table 4.1b: Average short-term direct cost of 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
Mean cost	£3,110	£3,040	£4,020	£18,800
Median cost	£0	£0	£0	£0
Base	170	97	73	62

We defined long-term direct costs, shown in Table 4.2, as external payments in the aftermath of the breach or attack incident.

The examples included in the survey were:

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

Table 4.2a: Average long-term direct cost of 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
Mean cost	£500	£460	£1,210	£320
Median cost	£0	£0	£0	£0
Base	968	640	328	423

Table 4.2b: Average long-term direct cost of 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
Mean cost	£2,950	£2,820	£5,020	£1,930
Median cost	£0	£0	£0	£0
Base	164	94	70	63

We also asked about the costs of any staff time (i.e., indirect costs of the breach or attack), as displayed in Table 4.3. This includes, for instance, how much staff would have got paid for the time they spent investigating or fixing any problems caused by the breach or attack. We explicitly asked respondents to include the cost of this time regardless of whether this duty was part of the staff member's job function or not.

Table 4.3a: Average staff time 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
Mean cost	£480	£460	£960	£140
Median cost	£0	£0	£30	£0
Base	970	639	331	410

Table 4.3b: Average staff time 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
Mean cost	£2,050	£1,980	£3,230	£540
Median cost	£100	£100	£180	£40
Base	172	98	74	59

Finally, as Table 4.4 shows, we asked about other indirect costs related to breaches, including the following areas (offered as examples to respondents):

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

Table 4.4a: Average indirect 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
Mean cost	£120	£110	£350	£130
Median cost	£0	£0	£0	£0
Base	986	642	344	419

Table 4.4b: Average indirect 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
Mean cost	£620	£570	£1,340	£820
Median cost	£0	£0	£0	£0
Base	172	98	74	61

Table 4.5 combines the estimates across all the areas of costs covered in the survey (direct costs, staff time and other indirect costs). The figures here can be considered the average total cost that organisations have faced from their single most disruptive breach.

Table 4.5a: Average 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
Mean cost	£1,600	£1,510	£3,350	£3,240

Across organisations identifying any breaches or attacks	All businesses	Micro/small Businesses	Medium/large businesses	All charities
Median cost	£0	£0	£30	£0
Base	1,006	652	354	425

Table 4.5b: Average 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
Mean cost	£8,260	£7,960	£12,560	£21,540
Median cost	£370	£370	£1,150	£200
Base	181	101	80	63

Commentary on the financial costs

The following key findings should be noted from these cost tables (Tables 4.1 to 4.5):

- among businesses identifying breaches with an outcome, the immediate direct costs of a cyber security breach or attack (Table 4.1b) were reported as very similar to the longer-term costs in the aftermath of an incident (Table 4.2b). This was different to 2024, 2023 and 2022 where for micro and small businesses short-term direct costs were recorded as being much higher than longer-term costs.
- the mean average total cost of the most disruptive breach for businesses (of all those identifying breaches or attacks regardless of whether there was an outcome) remained similar, but slightly higher than 2024 where it was £1,205 (compared to £1,600 this year). The mean average cost for those with an outcome was also slightly higher this year (£8,260) compared to in 2024 (£6,940).
- for long-term direct cost and average staff time cost, businesses tended to have higher costs than charities, in line with 2024. However, this year

on short-term direct costs and indirect costs of the most disruptive incident (both across all organisations identifying breaches and attacks and only organisations with an outcome), the cost for charities was higher than for businesses. This was due to one particularly high response given at this question by a single charity of £350,000[footnote 15]. This made the average total cost of the most disruptive breach or attack for charities (£3,240 across all breaches and attacks and £21,540 across those with an outcome) much higher than in 2024 (£460 across all breaches and £1,850 across those with an outcome).

- the median cost across all businesses and charities (whether they had experienced an outcome or not) for all costs was typically £0. This was also a similar pattern to previous years. This reflected the fact that, for most breaches or attacks, organisations do not identify any material outcome, so do not always recognise the need for a response. An area of exception, where the median cost was not £0, is the staff time cost among medium and large businesses, which suggests that even for those incidents that do not have a specified outcome, some staff time was still needed in dealing with it.

Table 4.6 shows the same average total self-reported cost estimate of the most disruptive breach or attacks as in Table 4.5 but excludes 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 are higher among this group.

Table 4.6a: Average 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
Mean cost	£3,550	£3,400	£5,590	£8,690
Median cost	£170	£170	£270	£170
Base	512	299	213	194

Table 4.6b: Average 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	Medium/large businesses	All charities
Mean cost	£10,140	£9,830	£14,360	£29,520
Median cost	£600	£590	£1,410	£500
Base	154	85	69	50

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 30% 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 form of action following a cyber breach or attack continued to revolve around internal reporting, to directors (76% of businesses and 80% of charities) or keeping an internal record of the incident (58% of businesses and 69% of charities).
- External reporting was still uncommon - among those identifying breaches or attacks, as around four in ten businesses (39%) and a third

of charities (33%) reported their most disruptive breach outside their organisation.

- Larger organisations were more likely to put in place a number of response measures following a cyber breach or attack and to have an incident response plan (53% of medium businesses and 75% of large businesses), as were those in the health, social care or social work sector (66%), finance or insurance sector (50%) and the information or communication sector (43%).
- Whilst typically stable at the overall level for businesses and charities, small businesses have seen significant increases in implementing incident response since 2024, including guidance on internal reporting (55% up from 48% in 2024), communications plans (29% up from 21% in 2024) and guidance on external reporting (48% up from 41% in 2024) .
- The most common preventative measure adopted following a breach or attack was additional staff training (32% of businesses and 38% of charities), with likelihood to take some form of action to prevent future breaches and attacks increasing with organisation size.

5.1 Incident response

Figure 5.1 shows the actions organisations said they take, or would take, in response to a cyber incident, using a prompted list. By far the top response was to inform senior management. It was far less common for organisations to say they would inform regulators. This is 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 (15% businesses and 11% charities).

Of those that had cyber insurance, just over half of businesses (52%) and charities (56%) 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

Action	Businesses	Charities
Inform your directors or trustees of the incident	76%	80%
Keep an internal recordof incidents	58%	69%
Assess the scale and impact of the incident	56%	63%

Action	Businesses	Charities
Formal debriefs or discussions to log any lessons learnt	54%	62%
Inform your cyber insurance provider (among those with insurance)*	52%	56%
Inform a regulator of the incident when required	47%	55%
Attempting to identify the source of the incident	45%	48%
Use an NCSC-approved incident response company	15%	11%

Bases: 2,180 businesses; 1,081 charities. *Only asked of those that have cyber insurance (554 businesses, 244 charities)

Figure 5.2 shows the documentation, guidance and processes that organisations have in place for such incidents. While a large majority of organisations said in Figure 5.2 that they would take several actions following a cyber breach or attack, in reality a smaller proportion already had processes in place to support this. The most common processes, mentioned by around a third of businesses and charities, included having specific roles and responsibilities assigned to individuals (39% of businesses and 34% of charities), having guidance on internal reporting (34% of businesses and 31% of charities) and having guidance on external reporting (32% of businesses and 30% of charities). Incidence of formal incident response plans was lower, with around two in five having one in place (23% of businesses and 22% of charities).

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

Action	Businesses	Charities
Roles or responsibilities assigned to individuals during or after incident	39%	34%
Written guidance on who to notify	34%	31%
Guidance for when to report externally (e.g. to regulators or insurers)	32%	30%
Formal incident response plan	23%	22%

Action	Businesses	Charities
External communications and public engagement plans	16%	15%

Bases: 2,180 businesses; 1,081 charities

Larger organisations were more likely than average to say they would have, or already had in place, each of the measures in Figures 5.1 and 5.2. For example, 53% of medium-sized businesses, 75% of large businesses and 45% of high-income charities had a formal incident response plan.

Three sectors tended to have a more formalised cyber incident response approach. They were significantly more likely than businesses overall to have a number of measures shown in Figure 5.2, and in particular, they were more likely than businesses overall (23%) to have an incident response plan:

- Health or social care sector (66% have an incident response plan)
- Finance or insurance sector (50% have an incident response plan)
- Information or communication sector (43% have an incident response plan).

Trends over time
Whilst the proportion of charities and businesses overall implementing response measures has remained stable with 2024, small businesses have seen significant increases across various response measures. This included guidance on who to notify (55% compared with 48% in 2024), external communications and public engagement plans (29% compared with 21% in 2024), and guidance on external reporting (48% compared with 41% in 2024).

Qualitative insights on the challenges around incident response
The qualitative interviews highlighted several challenges organisations might face when dealing with cyber incidents. Smaller organisations were often reliant on Digital Service Providers (DSPs), such as IT providers and cloud storage providers, for incident response. These organisations saw their DSP as the first port of call should a cyber security incident occur, and found them to be a source of advice and guidance following such incidents. In some cases all responsibility for cyber security had been delegated to these providers, which led to a lack of any formal internal processes.

> “My view is that if we’re paying them for a service, then it is their responsibility to ensure they deliver a service. And I’m not that

> concerned about the means by which they achieve it. I'm interested in outcomes, not in process." **Head of IT, Medium business**

> "We have a service provider that we use and they've got the skills, so we do utilise them as a consultant and we do also have another company who do the penetration testing or the testing of the emails and phishing and all that kind of stuff. I've got a level of consultancy with them on elements of that as well." **IT Lead, Medium business**

Smaller organisations also found it harder to develop incident response plans, because of a lack of in-house expertise or capacity. The unpredictability of cyber incidents added to this problem, with smaller organisations sometimes feeling helpless against the countless possible breaches or attacks that could take place and that were hard to prepare for in the event of not having experienced them previously. Smaller businesses also typically admitted to infrequent testing of their incident response plans, often conducting tests only after experiencing a breach. Furthermore, some businesses expressed uncertainty about the precise steps to take should a breach occur.

> "Then after [contacting a bank] I'd probably go into a major panic and not know who to contact." **General manager, Small business**

Tighter budgets and team capacity were also a challenge for organisations, particularly at the smaller end, when preparing for cyber security attacks. In larger organisations, the challenges were often more related to a disconnect between IT or cyber teams and wider staff, including senior managers.

Larger businesses typically reported higher frequencies of incident testing, ranging from daily to yearly and some of the medium and large organisations had simulation exercises and scenario tests in place to identify any weak spots in their staff training and preparedness. However, lack of staff buy-in to these exercises was often cited, with a feeling that staff did not want to devote time to partaking in the exercises.

Several medium and large organisations did report that their IT teams were well prepared for a cyber incident and in a number of cases guidance had been obtained from the NCSC.

Some businesses that conducted tests mentioned doing so at the suggestion of their insurance providers, either as a requirement or in preparation for an audit.

> "When we had a cyber-attack in February earlier this year, we were led by the insurance companies' external IT firm and their auditing and set requirements of things to do." **IT manager, Medium business**

It was also mentioned by some that they avoided overly frequent incident testing to prevent incident response from becoming too routine or predictable.

> "We've had a fair few over the last few months. Obviously, you don't want to keep it too regular. The people will know what to look out for now." **Customs specialist, Medium business**

Charities mentioned testing either yearly or not at all and generally demonstrated lower awareness of incident planning, with breaches or attacks often prompting testing rather than proactive planning.

Ransomware payments
Around half of businesses (52%) and four in ten charities (38%) had a rule or policy to not pay ransomware demands, which was consistent with 2024 (businesses 48% and charities 37%). However, there was still a high level of uncertainty among organisations on this topic, with one in five businesses (20%) and one in four charities (25%) saying they did not know what their organisation's policy on this was.

Findings were largely similar by size and sector, although businesses in the information or communication sector were more likely than average to say they had a rule not to pay out ransom demands (75% compared with 52% overall).

5.2 External reporting of breaches or attacks

External reporting of breaches was not widespread among organisations. This year, among those identifying breaches or attacks, around four in ten businesses (39%) and a third of charities (33%) reported their most disruptive breach outside of their organisation.

As in previous years, many of these cases simply involved organisations reporting breaches to their external cyber security or IT providers and no one else. When excluding these, we found that a quarter of these businesses (25%) and one in five of these charities (21%) that had identified a breach or attack reported them externally. Figure 5.3 shows the top places, beyond cyber security or IT providers, that businesses and charities

tended to report breaches externally. To note, this question was unprompted in both the telephone and online surveys.

Figure 5.3 serves to highlight the important role played by banks (21%) and internet and network providers (20%) for businesses, while for charities the top two ports of call for reporting disruptive breaches were internet and network providers (22%) and the police (16%).

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)

Reported to	Businesses	Charities
Bank building society or credit card company	21%	12%
Internet/Network Service Provider	20%	22%
Suppliers/business partners	11%	5%
Other government agency	9%	12%
Police	9%	16%
Outsourced cyber security provider	7%	8%
Action Fraud	6%	3%
Antivirus company	5%	0%
Clients/customers	4%	5%
Social media site (e.g. Facebook)	4%	4%
Website administrator	4%	3%
National Cyber Security Centre (NCSC)	4%	2%
Professional/trade/industry association	3%	1%
Information Commissioner’s Office (ICO)	2%	5%
Other	8%	14%

Bases: Those that reported their most disruptive breach externally (to someone other than an outsourced cyber security or IT provider, or a parent company): 238 businesses; 90 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 81% of charities this was the case). Beyond this, the next most common reasons were:

- they did not know who to report to (11% of businesses and 9% of charities)
- they did not think reporting would make any difference (5% businesses and 4% charities)
- they did not think reporting would lead to a benefit for their organisation (5% businesses and 4% charities).

Qualitative insights as to why organisations may not report breaches
The qualitative interviews examined organisations' experiences of reporting breaches externally. Whilst some organisations had detailed incident response plans, others dealt with incidents in a more ad-hoc or reactive manner. In these instances, a specific member of staff would typically use their discretion as to whether the incident needs to be reported or dealt with formally. Furthermore, as touched on previously, some organisations who were reliant on their DSPs for IT support would defer cyber security incidents to them.

When breaches did occur, businesses and charities generally viewed reporting breaches or attacks favourably. However, there were some discrepancies regarding the criteria for reporting and who this meant reporting to. Some businesses notified board members of all potential incidents, while others only notified them of successful or serious breaches or attacks.

When considering the circumstances in which incidents should be reported externally, this depended on the scale or seriousness of the breach. For example, breaches that involved disclosure of personal information were generally seen as requiring external reporting. Reputation was also considered in the decision-making process of whether to report, with one business citing that any attack could have an impact on reputation if not reported properly.

> "So any attack, whether it's a cyber security one or even just a technical failure, has the same impact on reputation, on repeat business, on people recommending us." **Head of IT, Medium business**

External reporting was often linked to the ICO, banks, or insurance companies. Charities demonstrated a greater propensity to report cyber incidents, implying this was due to caution and concerns about potential

repercussions for under-reporting. One charity suggested that they may prioritise cyber transparency over efficiency.

Some respondents acknowledged the potential long-term benefits of reporting to Action Fraud, citing increased awareness and broader visibility that could benefit other organisations. However, many did not consider Action Fraud or police involvement crucial for individual cyber breach mitigation, with some expressing unfamiliarity with Action Fraud altogether.

> "On a positive outcome, law enforcement would have a better understanding of how often it's happening. So I would say it's more positive to report it because then everybody's aware of what's going on." **IT manager, Medium business**

> "It depends on how much time [Action Fraud] take away from us. Being able to resolve the incident at hand." **Head of IT, Medium business**

5.3 Actions taken to prevent future breaches or attacks

Among those that identified any breaches or attacks, 62% of businesses and 67% 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 (32% businesses, 38% charities).

Likelihood to take some form of action to prevent future breaches and attacks increased with organisation size. Small (69%), medium (78%) and large (82%) businesses were all more likely than micro businesses (60%) to have taken some form of action. Likewise, high-income charities (84%) were more likely to have taken some kind of action compared to charities overall (67%).

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

Action taken	Businesses	Charities
People or training changes (such as staff training or communications)	32%	38%

Action taken	Businesses	Charities
Technical changes (such as updated antivirus software)	30%	33%
Governance changes (such as increased monitoring)	8%	6%
Any action taken	62%	67%
No action taken	36%	31%

Bases: Those that were able to specify a breach or attack experienced in the last 12 months: 1,032 businesses, 429 charities

As may be expected, the picture changed slightly when looking only at the organisations whose most disruptive breach resulted in a material outcome (e.g. the loss of files, money, or other assets). Figure 5.5 shows that the proportion who took some form of action rose to eight in ten businesses (79%) and charities (80%). Among those who had an outcome, making technical changes such as getting updated antivirus software or updating firewall systems became the most common response (56% businesses and 56% charities who had a breach or attack and had an outcome). A sizeable minority was left that did nothing in the event of a breach or attack that led to an outcome (17% businesses and 14% 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

Action taken	Businesses	Charities
Technical changes (such as updated antivirus software)	56%	56%
People or training changes (such as staff training or communications)	24%	33%
Governance changes (such as increased monitoring)	16%	10%
Any action taken	79%	80%
No action taken	17%	14%

Bases: Those that were able to specify a breach or attack experienced in the last 12 months and had an outcome: 190 businesses, 65 charities

Qualitative insights on cyber security data protection
Businesses and charities generally seemed to be aware of how the impact of cyber breaches and attacks related to data protection processes. Encryption, particularly Microsoft encryption, was a common cyber security method applied to combat data protection risks from cyber breaches.

> "Everything's encrypted, 365 provides encryption and we use end-to-end encryption for most of our messaging which is now done on Microsoft Teams." **CEO, Charity**

Multi-factor authentication seemed to be an increasingly common way of protecting data. Businesses and charities also noted the importance of restricting access to data, disposing of data, and following strictly defined processes for sharing data securely.

> "It's not just a case of keeping the data safe when you're working on a project. It's also the safe disposal of that. And we have to prove that. And only certain personnel are allowed access to that data while we're working on it." **General manager, Small business**

> "Where we can we anonymise where we encrypt all personal data at rest or in transit. … we have strict procedures around sharing personal information and other business confidential information with third parties… There are defined processes for sharing it securely." **IT manager, Charity**

When breaches or attacks did occur, businesses and charities generally viewed reporting incidents or breaches favourably, however, there were some discrepancies regarding the criteria for reporting. Some businesses notified board members of all potential incidents, while others only notified them of successful or serious breaches. Some businesses employed formalised approaches to assess the severity and reportability of a breach, while others relied on informal approaches. One smaller business reported losing a small number of customers after notifying them of a potential breach, rather than an actual breach. This highlighted the importance of reputational considerations when deciding whether to report a breach.

> "So any attack, whether it's a cyber security or a doctor failure or even just a technical failure, has the same impact on reputation, on repeat

> business, on people recommending us." **Head of IT, Medium business**

Charities typically stated that they would report most cyber incidents. One charity mentioned a tendency to over-report, suggesting that charities may prioritise cyber transparency over efficiency, or harbour concerns that under-reporting could negatively impact their reputation.

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 16]. 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 (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).

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 20% of businesses and 14% of charities have been the victim of at least one cyber crime in the last 12 months, accounting for approximately 283,000 businesses and 29,000 registered charities.
- The larger the business, the more likely they were to experience cyber crime (18% of micro businesses, 25% of small businesses, 43% of medium businesses and 52% of large businesses). The same pattern was evident among charities with likelihood to experience cyber crime increasing with income (11% of low-income charities, 18% of medium-income charities, and 38% of high-income charities).
- The prevalence of cyber crime overall among businesses and charities remained consistent with 2024 (20% businesses in 2025 and 22% businesses in 2024 and 14% in both years for charities), as did non-phishing related cyber crime for businesses (4% in 2025 and 3% in 2024) and charities (3% in 2025 and 2% in 2024).
- Whilst the prevalence of cyber crime overall remained static, the prevalence of ransomware among businesses has significantly increased between 2024 and 2025. The estimated percentage of all businesses who experienced a ransomware crime in the last 12 months increased from less than 0.5% in 2024 to 1% in 2025, which equates to an estimated 19,000 businesses in 2025.
- Phishing cyber crime remained by far the most common type of cyber crime experienced (93% of businesses and 95% of charities that experienced a cyber crime).
- Businesses who were victims of cyber crime experienced an average of 30 cyber crimes of any kind, in the last 12 months, whereas for charities this was 16. For both business and charities the median was 4 cyber crimes. This indicates a high level of repeat victimisation amongst some organisations experiencing cyber crime.

- It is estimated that UK businesses have experienced approximately 8.58 million cyber crimes of all types including approximately 680,000 non-phishing cyber crimes in the last 12 months. UK charities have experienced approximately 453,000 cyber crimes of all types in the last 12 months.
- The average self-reported cost per business associated with cyber crime (excluding phishing) experienced in the last 12 months was a mean average of £990 including £0 responses (and £1,970 excluding £0 responses).
- For around 3% of businesses and 1% of charities, cyber breaches or attacks are seen to facilitate fraud, equating to approximately 40,000 businesses and 2,000 charities. There were an estimated 72,000 cyber-facilitated fraud events across the UK business population in the last 12 months.
- Self-reported costs associated with cyber-facilitated fraud experienced in the last 12 months were higher than for cyber crime, with an estimated mean average cost of £5,900 per business including those giving a cost of £0 (and £10,000 where £0 responses are excluded).

6.1 Note on comparability to previous year

The cyber crime questions were introduced in the 2023 survey. However, the cyber crime and cyber-facilitated fraud questions in the 2024 questionnaire were changed to strengthen the reliability of the data from 2023, based on feedback from the Home Office and from cognitive testing completed in 2024. This meant that cyber crime results could not be compared between 2023 and 2024.

This year in 2025, whilst the cyber crime section remains experimental, the questionnaire remains largely in line with that used in 2024. Some changes have been made to the wording of questions that feed into the ransomware cyber crime figures to aid understanding[footnote 17], but the changes made do not represent a substantive difference in the way cyber crime has been recorded. On this basis, we are able to compare this year's cyber crime results against the 2024 baseline.

The questionnaire changes for 2025 also included some edits to the questions used to obtain cyber-facilitated fraud estimates. The questions were changed to ask organisations to specifically include instances of fraud that were related to or as a result of phishing attacks. On this basis we are unable to directly compare cyber-facilitated fraud estimates, including prevalence and cost, to 2024.

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-2025/cyber-security-breaches-survey-2025-technical-report).

6.3 The prevalence of cyber crime

Looking across all the different types of cyber crime, we estimate that 20% 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 283,000 businesses and 29,000 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 30% of charities identifying any cyber security breaches or attacks, just under half (46% of businesses and 48% 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 (18%) have experienced cyber crime in the last 12 months, the same was true for a quarter of small businesses (25%), around two in five medium businesses (42%) and around half of large businesses (52%). 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 that have experienced any cyber crime in the last 12 months, over time

Business type	2025	2024
Micro businesses	18%	19%
Small businesses	25%	29%
Medium businesses	42%	45%
Large businesses	52%	58%
Businesses overall	20%	22%

Bases: 2025: 1,013 micro businesses; 565 small businesses; 413 medium businesses; 188 large businesses; 2,179 businesses overall. Bases: 2024: 1,060 micro businesses; 506 small businesses; 264 medium businesses; 170 large businesses; 2,000 businesses overall

As shown in Figure 6.1, the prevalence of cyber crime among businesses overall and by business size remains consistent with 2024, with no significant changes. The largest difference can be seen among large businesses where the proportion of businesses experiencing a cyber crime was 58% in 2024 and is now 52% in 2025, however as with all business sizes, this does not constitute a significant difference. This is unlike the trend for breaches and attacks seen in Chapter 4, where a decrease in breaches and attacks was seen among micro and small businesses.

When examining non-phishing related cyber crime experienced among businesses in the last 12 months (4%), there was also no significant change from 2024 (3%).

Looking at cyber crime experienced by business sector (Figure 6.2), those in the information or communications (43%) and the administration or real estate (26%) sectors were significantly more likely than businesses overall (20%) to experience a cyber crime. There were some differences in the business sector trends amongst those reporting breaches or attacks as opposed to cyber crime. Whilst the information or communications sector was more likely than businesses overall to experience a breach or attack more generally (69% compared to 43% for businesses overall), the administration or real estate sector was not significantly more likely than businesses overall to experience a breach or attack (48% compared to 43% businesses overall).

Businesses in the food or hospitality (12%) and retail or wholesale (11%) sectors were less likely than businesses overall (20%) to experience a cyber crime, reflecting the pattern of those less likely to experience a breach or attack.

The proportion of businesses in the retail or wholesale sector experiencing a cyber crime has decreased significantly (from 18% in 2024 to 11% in 2025). There were no other significant differences observed among sectors between 2024 and 2025.

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

Industry sector	
Information or communications	43%
Administration or real estate	26%
Professional, scientific or technical	25%
Finance or insurance	24%
Utilities or production	23%
Health or social care	22%
Entertainment or service	20%
Construction	17%
Transport or storage	17%
Food or hospitality	12%
Retail or wholesale	11%
Businesses overall	20%

Bases: 130 information or communications businesses; 320 administration or real estate businesses; 273 professional, scientific or technical businesses; 141 finance or insurance businesses; 150 utilities or production businesses; 150 health or social care businesses; 100 entertainment or service businesses; 231 construction businesses; 94 transport or storage businesses; 168 food or hospitality businesses; 357 retail or wholesale businesses; 2,179 businesses overall

In addition, businesses in London were more likely than businesses overall to experience a cyber crime in the last 12 months (27% in London compared to 20% overall). However, it is worth noting that regional analysis of prevalence will be influenced by other factors, such as the distribution of business sectors.

As outlined in Figure 6.3, and similar to the pattern for cyber security breaches and attacks more generally, likelihood of charities to experience a cyber crime increased with income (11% of low-income charities, 18% of medium-income charities, and 38% of high-income charities).

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

Charity type	2025	2024
Low-income charities	11%	10%
Medium-income charities	18%	21%
High-income charities	38%	37%
Charities overall	14%	14%

Bases: 2025: 446 low-income charities, 292 medium-income charities, 343 high-income charities; 1,081 charities overall. Bases: 2024: 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.

As with businesses, non-phishing related cyber crime experienced among charities in the last 12 months has also remained in line with 2024 (3% of charities in 2025 and 2% of charities in 2024).

The next section (Section 6.4) covers the types of cyber crimes that organisations faced. It is worth noting that most of the 20% 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 4% of businesses and 3% of charities have experienced at least one non-phishing cyber crime in the last 12 months. This amounts to approximately 51,000 businesses and 6,000 registered charities.

Similarly to all cyber crimes, non-phishing cyber crimes are more prevalent than average among large businesses (15% for large businesses compared with 4% of businesses overall) and high-income charities (6% compared with 3% of charities overall).

6.4 The nature of cyber crimes experienced

Figure 6.4 details the types of cyber crimes that organisations have faced, among the 20% 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 95% of charities that experienced a cyber crime having experienced phishing. This equates to 18% of all businesses and 14% of all charities.

As well as being more likely to experience cyber crime overall, businesses in London were more likely to experience phishing cyber crime (25% of all businesses in London) compared to businesses overall (18% of all businesses).

Hacking[footnote 18] was the second most common type of cyber crime, experienced by 8% of businesses and 17% of charities who experienced some type of cyber crime. This equates to 2% of all businesses and 2% of all charities experiencing hacking cyber crime.

Ransomware cyber crime was experienced by 7% of businesses who were the victim of a cyber crime (and equates to 1% of all businesses), but was rare among charities (less than 0.5% of charities who experienced a cyber crime). The other cyber crimes - viruses, spyware or malware and denial of service, were rare among businesses and charities.

Among businesses experiencing cyber crimes relating to unauthorised access, online takeovers or denial of service, 5% experienced some form of extortion, i.e. the attackers demanded a payment to end the breach or attack in question.

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

Type	Businesses	Charities
Phishing attacks	93%	95%
Hacking (unauthorised access or online takeovers)	8%	17%
Ransomware*	7%	0%

Type	Businesses	Charities
Viruses, spyware or malware	2%	3%
Denial of service	2%	1%

Bases: Those that identified a cyber crime: 613 businesses; 228 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%”.

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, will be 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	Estimated number of businesses that experienced cyber crime	Estimated number of charities that experienced cyber crime
Base	2,179	1,081
Phishing	261,000	28,000
Hacking	23,000	5,000
Ransomware	19,000	-
Viruses, spyware or malware	7,000	1,000
Denial of service	6,000	-

‘-’ denotes that for charities experiencing ransomware and denial of service cyber crimes the estimates were too low to produce extrapolations.

It is worth noting that there is a drop between the number of organisations reporting ransomware as a breach or attack, (3% of all businesses[footnote 19], which equates to approximately 37,000 businesses) and the number who experienced a ransomware cyber crime (1% of all businesses, which

equates to 19,000 businesses). This mimics the pattern found in 2024 and among charities.

In 2024, to address the discrepancy between the two figures, wording around the ransomware question was amended for 2025. Rather than talking about ransomware in terms of 'successful' and 'unsuccessful' attacks in whether they had overcome internal or third-party software (as had been asked in 2024), it was changed in 2025 to ask about instances where a financial ransom was demanded. However, a similar discrepancy has emerged whereby a number of businesses and charities say at Q53A they have experienced their 'organisation's devices being targeted with ransomware, i.e. a type of malware that tells you to pay a ransom to restore your files or stop them being made public' but then when asked in how many of the ransomware attacks a financial ransom was demanded, roughly half say 'none' or they 'do not know'[footnote 20]. This leads to just under half of those selecting ransomware at Q53A being classified as having experienced a ransomware crime. It seems that on first asking, organisations can perceive they have been targeted with ransomware, but in the event of being probed further, it does not always involve a financial ransom being demanded. One possible explanation for this might be that some organisations are able to identify and block against a ransomware attack at an early stage, before a ransom is demanded.

Trends over time
Prevalence of the different types of cyber crime has remained largely consistent with 2024. The exception was among ransomware cyber crimes, which has seen a significant increase from less than 0.5% of all businesses in 2024 to 1% of all businesses in 2025. When looking at the number of businesses experiencing ransomware crime as a percentage of businesses experiencing any cyber crime, this equates to 2% in 2024 and 7% in 2025, which was also a significant increase.

There were no other significant changes in type of cyber crime experienced between 2024 and 2025, 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 20% 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 around a third (31%) of businesses experiencing cyber crime only identified 1 cyber crime in the last 12 months,

a sizeable minority were persistently targeted (23% experienced between 11 and 99 cyber crimes and 8% experienced 100 or more cyber crimes). The same was true for charities, where 16% of charities who identified a cyber crime in the last 12 months experienced between 11 and 99 cyber crimes and 7% 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

Organisation Type	% 1 cyber crime	% 2-10 cyber crimes	% 11-99 cyber crimes	% 100+ cyber crimes
Businesses	31	39	23	8
Charities	26	52	16	7

Bases: Those experiencing any cyber crime in the last 12 months: 613 businesses, 228 charities

On average (taking the mean estimates), businesses experienced 30 cyber crimes of any kind in the last 12 months and charities experienced 16. The median result, which may be more reflective of the typical organisation, suggested 4 cyber crimes in the last 12 months for both businesses and charities.

This data indicates a high level of repeat victimisation amongst some organisations experiencing cyber crime. This is still the case when looking at non-phishing related crime, but to a much lesser extent. Among the 4% of businesses identifying non-phishing cyber crimes, the mean average was 13 and the median average was 1.[footnote 21]

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.

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

- UK businesses have experienced approximately 8.58 million cyber crimes of all types including approximately 680,000 non-phishing cyber crimes in the last 12 months

- UK charities have experienced approximately 453,000 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 22], we estimate that:

- UK businesses have experienced approximately 7.87 million phishing cyber crimes and 595,000 hacking cyber crimes in the last 12 months
- UK charities have experienced approximately 442,000 phishing cyber crimes in the last 12 months

6.6 Financial cost of cyber crimes

Table 6.2 shows the estimated self-reported costs organisations incurred from all the identified cyber crimes over the past 12 months. This excludes cyber crimes where the only activity was phishing, i.e. where there was no follow-on crime from the phishing email, such as a successful ransomware attack or hacking. Where the phishing did lead to a follow-on crime, the cost of this – in theory - should be captured in the follow-on crime types.

Due to small sample sizes, it is not possible to break down these figures by the size of business (as is 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 is 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.

The wide gap between mean and median costs highlights that, just as with all cyber security breaches or attacks, the typical business faces relatively low costs. The range of costs experienced was wide, from less than £100 up to over £50,000, suggesting that a minority of businesses face potentially high costs from cyber crime.

Table 6.2: Average self-reported cost per business of all cyber crimes (excluding phishing) experienced in the last 12 months[footnote 23]

	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)
Mean cost	£990	£1,970
Median cost	£20	£600
Base	114	61

Average cyber crime costs this year were similar to in 2024[footnote 24], where the mean average cost including those giving a cost of £0 was £1,120 and the mean average cost excluding those giving a cost of £0 was £1,720.

As in 2024, in 2025 the mean average cost for the most disruptive cyber attack or breach was higher (£1,600 for all businesses identifying a breach or attack, including costs of £0) than the average cost of cyber crime (£990 for all businesses experiencing any cyber crime other than phishing, including costs of £0). The assumption has previously been that for phishing attacks with no follow-on cyber crime the cost will be negligible, however, we see repeatedly that phishing is deemed the most disruptive type of attack and findings from the qualitative interviews highlight that organisations can spend significant time dealing with large volumes of phishing attacks and investigating them (even when no crime has occurred, or the attempt was unsuccessful). Please see Section 4.4 for more insights on this from the qualitative interviews.

This provides some suggestion as to why phishing attacks may have costs associated with them, that are then captured in the survey under costs for the most disruptive breach or attack. Furthermore, the cost of phishing cyber crimes are not captured in the survey, which could be a reason for them being lower. The cyber-facilitated fraud cost estimates (included for businesses in Section 6.8) do include instances of fraud that resulted from a phishing attack, and are higher than both the average most disruptive breach or attack cost and the average cyber crime cost.[footnote 25]

6.7 Cyber-facilitated fraud

Prevalence of cyber-facilitated fraud

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 40,000 businesses and 2,000 charities.

The questions to obtain cyber-facilitated fraud estimates this year were edited 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 2024.

Scale of cyber-facilitated fraud

Amongst the 3% of businesses that experienced cyber-facilitated fraud, around six in ten (63%) said this happened just once in the last 12 months. The average (mean) number of cyber-facilitated frauds experienced by these businesses was 2 per business, with the median equating to 1 cyber-facilitated fraud per business.

As with the scale of cyber crime estimates (see Section 6.5), it is 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 72,000 cyber-facilitated fraud events across the entire business population in the last 12 months.

The sample size was too low (26) 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, 54% said this resulted from a phishing attack. After phishing attacks, the most common enablers of cyber-facilitated fraud were hacking or attempted hacking of online bank accounts (28%) and takeovers of organisation’s or user’s accounts (15%). 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

Type of breach or attack	% businesses affected
Phishing attacks	54%

Type of breach or attack	% businesses affected
Hacking or attempted hacking of online bank accounts	28%
Takeovers of organisation’s or users’ accounts	15%
Unauthorised accessing of files or networks by people outside your organisation	7%
Viruses, spyware or malware (excluding ransomware)	2%
Ransomware	1%
Denial of service attacks	1%
Unauthorised accessing of files or networks by staff or volunteers*	0%
Unauthorised listening into video conferences or instant messaging*	0%

Bases: 73 businesses that incurred fraud as a direct result of cyber breaches or attacks in the last 12 months

*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 6.3 outlines the average cost for businesses in the last 12 months of cyber-facilitated fraud. Again, the sample size was too low to include costs for charities. The questions to obtain cyber-facilitated fraud estimates this year were edited to specifically ask organisations to include fraud as a result

of phishing attacks, and are therefore not directly comparable with cyber-facilitated fraud costs from 2024[footnote 26].

The range of cyber-facilitated fraud costs experienced was wider than for cyber crime, ranging from less than £100 to more than £100,000, suggesting that a minority of businesses face potentially crippling costs from cyber-facilitated fraud.

Table 6.3: Average 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)
Mean cost	£5,900	£10,000
Median cost	£200	£500
Base	70	46

Chapter 7: Conclusions

The 2025 Cyber Security Breaches Survey reveals a complex and evolving cyber security landscape for UK businesses and charities. While larger organisations and specific sectors exhibit relatively mature cyber security practices, smaller organisations and certain sectors are less developed, highlighting persistent disparities and vulnerabilities.

Awareness and attitudes
Cyber security remains a high priority for the majority of businesses and charities, consistent with previous years. However, a trend has emerged that has seen board-level responsibility for cyber security steadily declining among businesses since 2021. Larger organisations demonstrated a higher prioritisation of cyber security, as observed in previous years.

While the overall proportion of organisations seeking external information or guidance remained stable, large businesses demonstrated a decrease on this measure.

Reliance on external cyber security consultants and IT providers remained the most common source of information, highlighting a potential gap in organisations' use of accessible and trusted guidance from official sources like the NCSC (National Cyber Security Centre).

Senior management involvement appears to be a decisive factor in advancing cyber security initiatives, as organisations with active senior leadership demonstrated more robust security strategies and controls. Despite this, there was a noted gap in the overall awareness and engagement with government-endorsed cyber security resources like Cyber Aware and Cyber Essentials.

Awareness of government initiatives like Cyber Aware, the 10 Steps guidance, and Cyber Essentials has seen a steady decline in awareness in recent years and remains fairly limited, particularly among micro businesses. Organisations tend to rely on external consultants and IT providers for information and guidance, potentially missing out on accessible and trusted resources from official sources. This perhaps suggests the importance of continuing to reiterate key messages and promote education on cyber security via official sources.

Approaches to cyber security

While small businesses are making progress in adopting cyber hygiene practices, high-income charities face challenges in maintaining momentum, potentially due to funding limitations.

Small businesses demonstrated improved adoption of key cyber hygiene practices, including risk assessments, cyber insurance, formal cyber security policies, and business continuity plans covering cyber security. This indicates a growing awareness of cyber risks and a proactive approach to risk mitigation among smaller businesses.

Conversely, high-income charities showed a decline in some key areas, including activities to identify cyber security risks, reviewing immediate supplier risks, and having a formal cyber security strategy. Qualitative insights suggested budget constraints as a potential limiting factor for charities.

Larger organisations benefit from formal strategies and established processes and were more likely to have formal cyber security strategies in place and to regularly review them. The majority of organisations have implemented basic technical controls, but there was room for improvement in adopting more advanced technical controls such as two-factor authentication, VPNs, and user monitoring remains lower than on other measures.

Prevalence of cyber breaches and attacks

While the overall prevalence of cyber breaches or attacks among businesses has decreased compared to 2024, the number of affected

organisations remains substantial (estimated 612,000 businesses). This decline is primarily attributed to fewer micro and small businesses reporting phishing attacks. Prevalence of cyber breaches and attacks remains high among medium and large businesses. For charities, the prevalence has remained stable since 2024, with an estimated 61,000 charities experiencing cyber breaches and attacks over the last 12 months.

Findings suggest tackling phishing may be key to helping guard against some of the most disruptive and costly impacts associated with cyber breaches and attacks. Phishing attacks remain the most prevalent and disruptive form of cyber breach or attack and the qualitative insights emphasised the time-consuming nature of addressing phishing incidents due to their volume, frequency and the requirement for staff training. The emergence of AI-powered impersonation as a sophisticated phishing method has added a new layer of complexity.

Further to this, phishing was also the most common enabler of cyber-facilitated fraud, which in itself was associated with some of the highest costs experienced by businesses. Robust defences and user education regarding phishing will therefore continue to be important.

While the proportion of organisations experiencing negative outcomes from breaches or attacks remained consistent with 2024, some specific outcomes vary. Businesses experienced a significant increase in temporary loss of access to files or networks, while charities saw a rise in loss of access to third-party services.

While the estimated average self-reported cost of the most disruptive breach or attack provides a benchmark from which to assess the financial impact of breaches or attacks, these averages mask the wide range of costs experienced, with many incidents having minimal direct financial consequences.

Dealing with cyber breaches or attacks

Internal reporting of breaches or attacks to senior management was common, but external reporting remains uncommon. The limited prevalence of external reporting suggests a potential reluctance to disclose incidents, highlighting the need to encourage transparent reporting and promote the benefits of information sharing.

Larger organisations and those in specific sectors like health or social care, finance or insurance, and information or communication, demonstrated more formalised incident response approaches.

While larger organisations have more formalised incident response procedures, smaller businesses are making progress in improving their incident response capabilities. Small businesses show a significant increase in implementing various incident response measures compared to 2024,

including guidance on internal and external reporting and communication plans.

Additional staff training was the most common preventative measure adopted following a breach or attack, perhaps highlighting organisations' understanding of the importance of ongoing education and awareness raising.

Cyber crime

The overall prevalence of cyber crime remains consistent with 2024, with higher prevalence among medium and large businesses and high-income charities.

While overall cyber crime prevalence was stable, there has been a significant increase in ransomware crimes when looking at both businesses overall and businesses that experienced cyber crime.

Phishing cyber crime remained the most common type of cyber crime, while other forms like hacking, ransomware, viruses, and denial of service attacks were less common.

The stable prevalence of cyber crime, despite a decrease in overall prevalence of breaches or attacks, suggests that organisations remain vulnerable to the most serious cyber breaches and attacks that ultimately end up recorded as cyber crime. Going forwards it would be useful to further explore and understand the differences in trends regarding breaches or attacks as compared to cyber crime.

Prevalence of both cyber breaches and attacks and cyber crimes in micro and small businesses was lower than in medium and large businesses. These findings may potentially indicate poorer identification and reporting practices in smaller organisations with less sophisticated cyber security monitoring in place. While several cyber security hygiene practices have improved for small businesses this year (as outlined in Chapter 3), they are still less likely than medium and larger businesses to undertake these behaviours.

Cyber-facilitated fraud, where a breach or attack leads to fraud, affects a small proportion of organisations, but associated costs (included in the report for the first time) are higher than for cyber crime. This provides insight into the facilitatory nature of cyber crime and the wide range of costs that this can incur on organisations.

Overall conclusion

The 2025 survey emphasises that while progress is being made in certain areas, evolving threats like phishing and ransomware, and disparities between different types of organisations highlight persistent vulnerabilities. The observed strengthening of cyber hygiene among small businesses, promoting official guidance and initiatives, improving incident response

capabilities, encouraging transparent reporting, managing supply chain risks, and empowering boards with cyber knowledge are all crucial steps toward building a more secure and resilient cyber landscape for the UK.

Appendix A: Guide to statistical reliability

The final data from the survey are based on weighted samples, to represent the entire population of UK businesses or charities with employees. Percentage results are therefore subject to margins of error, which vary with the size of the sample and the percentage figure concerned.

For example, for a question where 50% of the 2,180[footnote 27] businesses sampled in the survey give a particular answer, there is a 95% chance that this result would not vary by more or less than 2.7 percentage points from the true figure the 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 28]

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

	10% or 90%	30% or 70%	50%
2,180 businesses	±1.6	±2.5	±2.7
1,014 micro businesses	±1.9	±2.9	±3.2
565 small businesses	±2.6	±4.0	±4.3
413 medium businesses	±3.0	±4.6	±5.0
188 large businesses	±4.4	±6.7	±7.4
1,081 charities	±2.2	±3.4	±3.7

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 fraud	In the context of this study, we define fraud as being dishonest action, with the intent of making a financial gain at the expense 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).
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

Term	Definition
	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 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) are encrypted network connections, 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
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
- Nada El-Hammamy, Ipsos
- Eva Radukic, Ipsos
- Jono Roberts, Ipsos
- Hannah Harding, Ipsos
- Jayesh Navin Shah, Ipsos

2.The Cyber Security Breaches Survey was first published in 2016 (https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016) as a research report, and became an Official Statistic in 2017. The previous reports can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey (https://www.gov.uk/government/collections/cyber-security-breaches-survey). This includes the full report and the technical and methodological information for each year.

3.The lead DSIT analyst and responsible statistician for this release is Saman Rizvi. The lead Home Office analyst for this release is Eleanor Fordham. For enquiries on this release, please contact DSIT at cybersecurity@dsit.gov.uk.

4.The Cyber Security Breaches Survey is an official statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https://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.

5.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 1.7 of the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report)
2. This research was previously commissioned by the former Department for Digital, Culture, Media and Sport (DCMS). In February 2023, the parts of UK government responsible for cyber security policy moved to the new department, DSIT.
3. Fieldwork for the Cyber Security Breaches Survey took place in autumn and winter 2024, where organisations were asked about their cyber security experiences over the preceding 12 months. This data is referred to as 2025, which represents the year that the data is published. Preceding years of the survey followed a similar pattern, with the year referencing the year of publication and the majority of fieldwork typically taking place in the autumn and winter of the previous year.
4. The 2016 publication can be found here: Cyber Security Breaches Survey 2016 - GOV.UK (https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016) - 2017 to 2024 publications can be found here: https://www.gov.uk/government/collections/cyber-security-breaches-survey (https://www.gov.uk/government/collections/cyber-security-breaches-survey)
5. 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.
6. 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).

7. Further detail on significance testing is included in the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report) in Section 2.6.
8. 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-2025/cyber-security-breaches-survey-2025-education-institutions-findings).
9. These aggregated results (for organisations updating managers at least quarterly) across this section exclude the proportion of businesses and charities that say they update senior managers each time there is a breach (although these are still included in the base).
10. This is 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.
11. 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)
12. 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.
13. The * next to the base of 2,179 for businesses overall indicates that 1 micro business was not asked this question (Q53A) due to an unknown CATI script error that only affected this question and a single respondent. This means that they have been excluded from the base at this question, and any subsequent question that would have been routed dependent on their answer at Q53A, including all of the cyber crime questions. More detail on this is included in the separately published Technical Annex. (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report)
14. 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. (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report)

15. This interview was listened back to in order to verify that the response given was accurate, which it was. It was therefore kept in the data, despite being significantly higher than all other responses at this question.
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. Minor wording modifications at the questions on ransomware were made to increase the specificity of answers, changing the language from asking about ‘successful’ attacks that overcame internal or third-party software, to asking about ‘attacks where a financial ransom was demanded’
18. Wherever hacking is referred to throughout Chapter 6 it is referring to hacking including unauthorised access or online takeovers
19. This figure comes from Q53A where organisations were asked if they had experienced ransomware, but in this question it hadn’t yet been confirmed that this breach or attack involved a financial ransom being demanded.
20. On unweighted figures 95 organisations selected ‘ransomware’ breach or attack at Q53A. Three of these reported that the ransomware attack they had experienced led to fraud, which meant they were not eligible to go through to the cyber crime section of the questionnaire. When the remaining 92 were asked in how many of the ransomware attacks was a financial ransom demanded 45 said ‘0’ and 10 said they did not know. This left 37 organisations that answered at least one attack where a financial ransom was demanded, and this is the group classified as having experienced a ransomware cyber crime.
21. There were too few cases of non-phishing cyber crime among the sampled charities to report statistically reliable results
22. Other types of cyber crime extrapolations on scale can not be made due to insufficient base sizes of those experiencing the relevant cyber crime
23. As in Chapter 4, the cost estimates in Chapter 6 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. (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report)

24. No significance testing on costs was done between years, please see footnote 5 for more details.
25. No significance testing on costs was done between years, please see footnote 5 for more details.
26. Cyber-facilitated fraud costs were not published in 2024, but banded costs were included in the SPSS file on the UK Data Archive.
27. Where a base of 2,179 businesses is used (to account for the one micro business who did not get asked Q53A due to a script error) the same margins of error are apparent as noted for 2,180 businesses in Table A.1
28. 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 1,326 for businesses (compared with 1,398 in 2024, 1,702 in 2023 and 816 in 2022) and 685 for charities (compared with. 652 in 2024, 808 in 2023 and 267 in 2022)