2025

Cyber-security Breaches Survey

philip gibbs insurance brokers

Table of Contents

Introduction

The cyber-landscape is evolving at an unprecedented pace, becoming increasingly complex due to several key factors. Cyber-criminals are growing more sophisticated and leveraging advanced techniques and technologies. The rise of artificial intelligence (AI) attacks and organisations' increasing reliance on technology further complicate the situation. As threat actors continuously refine their evasion tactics, the importance of robust cyber-security defences has never been more critical.

The following report summarises data from the government's Cyber Security Breaches Survey 2025, commissioned by the Department for Science, Technology and Innovation as part of the National Cyber Security Programme. The figures within the survey illuminate areas where organisations could improve their cyber-security efforts.

As you read through the information, consider how your organisation could bolster its cyber-defences. Focus on identifying trends, evaluating cyber-security recommendations and applying best practices to mitigate risks.

Contact us today for further cyber-risk management and insurance solutions.

Please refer to the glossary to see how the government defines organisations of various sizes.

Overview of Findings

The number of businesses and charities reporting cyber-breaches this past 12 months has fallen slightly compared to last year's survey results, yet the cyber-threat landscape remains severe. Four in 10 (**43%**) businesses and 3 in 10 (**30%**) charities experienced a cyber-security breach or attack in the past 12 months, a decrease from **50%** and **32%**, respectively, in 2024. However, the decline was primarily driven by fewer micro and smaller businesses identifying phishing attacks, according to the government. The prevalence of cyber-breaches remains high in larger companies, with **67%** of medium and **74%** of large businesses experiencing at least one breach or attack this past year.

Across all organisations, phishing attacks—staff receiving fraudulent emails or being directed to fraudulent websites—remain the most prevalent and disruptive type of cyber-attack. Indeed, **85%** of businesses and **86%** of charities that fell victim to cyber-attacks were breached via phishing, and **65%** of businesses and **63%** of charities said their most disruptive breach was a phishing attack. Qualitative research from survey participants revealed organisations are concerned about the time-consuming nature of defending against phishing attacks, as well as the emergence of AI-powered impersonation, which makes phishing scams harder to spot.

Although the proportion of organisations experiencing a negative outcome from cyber-breaches in 2025 remained consistent with 2024's data, this year's survey found a statistically significant rise in organisations that lost access to files, networks and third-party services following a breach. These losses can severely hinder business operations; therefore, organisations should implement robust cyber-security measures to maintain operational continuity and lessen exposures.

Cyber-hygiene Measures

The survey revealed both positive and negative findings as it pertains to organisations' commitment to cyber-resilience. Consistent with the 2024 survey, cyber-security was a high priority for **72%** of businesses and **68%** of charities. Moreover, small businesses saw a notable uptick in cyber-hygiene measures, including risk assessment implementation, cyber-insurance uptake and continuity planning. However, increased cyber-hygiene activity was not universal; high-income charities saw a marked decline, possibly due to funding limitations. Furthermore, board-level responsibility for cyber-security is also declining; **38%** of businesses had a board member responsible for cyber-security in 2021, compared to just **27%** in 2025. Failing to prioritise cyber-security could leave organisations exposed to cyber-attacks and data breaches.

To defend against cyber-threats, most organisations have implemented basic technical controls, such as updated malware protection (**77%** of businesses, **64%** of charities), password policies (**73%** of businesses, **57%** of charities) and network firewalls (**72%** of businesses, **49%** of charities). However, fewer have adopted advanced controls, such as two-factor authentication (**40%** of businesses, **35%** of charities), virtual private networks (VPNs) (**31%** of businesses, **20%** of charities) and user monitoring (**30%** of businesses, **31%** of charities), suggesting there is room for improvement.

Overall, the varied uptake of cyber-hygiene measures among organisations and disparities between companies of different sizes could leave businesses and charities vulnerable to cyber-threats in the future. However, understanding the threat landscape can help organisations inform cyber-resiliency decisions and identify vulnerabilities.

Continue reading for further cyber-security insights.

Incidence and Impact of Cyber-incidents

This section summarises the data of businesses and charities that have experienced breaches or attacks in the past year and the impact of those events. It visually quantifies how many organisations have experienced a cyber-incident, which types of incidents were disruptive and the most common negative impacts that accompanied them.

Experience of Cyber-incidents

43% of businesses and **30%** of charities reported experiencing a cyber-breach or attack in the past 12 months. Among these organisations:

18% of businesses and **15%** of charities adopted new measures to prevent future attacks.

17% of businesses and **19%** of charities needed additional staff time dealing with the breach or attack.

11% of businesses and **11%** of charities stopped staff from carrying out their daily work due to the breach or attack.

Here is the frequency of breaches in the last 12 months broken down:

Among businesses that experienced a breach, **19%** experienced just one, **28%** experienced fewer than one per month, **23%** experienced one per month, and **29%** experienced one at least weekly.

Among charities that experienced a breach, **22%** experienced just one, **35%** experienced fewer than one per month, **21%** experienced one per month, and **18%** experienced one at least weekly.

The Most Disruptive Cyber-incidents

The most disruptive forms of cyber-attacks among organisations that reported more than one kind of attack in the past 12 months were:

Phishing attacks

(**65%** of businesses and **63%** of charities)

Others impersonating the organisation in emails or online

(**18%** of businesses and **20%** of charities)

Takeovers or attempted takeovers of website, social media or email accounts

(**4%** of businesses and **6%** of charities)

Impact of Breaches

16% of businesses and **16%** of charities that experienced a breach or attack reported suffering negative outcomes, such as:

Temporary loss of access to files or networks
(7% of businesses—up from 4% in 2024—and 5% of charities)

Website or online services taken down or made slower
(6% of businesses and 6% of charities)

Lost access to third-party services
(3% of businesses and 5% of charities—up from 1% in 2024)

Dealing with Cyber-incidents

This section displays information on how organisations handled breaches in the past 12 months. Specifically, this section visually represents the time organisations took to recover from a breach, the average costs of a disruptive data breach and actions taken by organisations following a cyber-attack.

Time Taken to Recover From a Cyber-incident

The average amount of time organisations took to get operations back to normal when dealing with their most disruptive breach in the last 12 months was as follows:

24 hours or less
(**92%** of businesses and **89%** of charities)

No time at all
(**77%** of businesses and **78%** of charities)

More than a day
(**8%** of businesses and **10%** of charities)

Financial Costs of Cyber-incidents

The average total costs (ie short- and long-term costs, both direct and indirect) of the most disruptive breach or attack in the past 12 months **among all organisations that reported a cyber-incident** were:

Businesses overall: £1,600

Medium and large businesses: £3,350

Charities overall: £3,240

The average total costs of the most disruptive breach or attack in the past 12 months **among organisations that reported an outcome to their cyber-incidents** were:

Businesses overall: **£8,260**

Micro- and small businesses: **£7,960**

Medium and large businesses: **£12,560**

Charities overall: **£21,540**

Understanding and Responding to the Cyber-incident

Only **23%** of businesses and **22%** of charities had a formal cyber-incident response plan. However, medium-sized businesses (53%), large businesses (75%) and high-income charities (45%) fared better.

Other common response measures were:

Informing senior management
(**76%** of businesses and **80%** of charities)

Keeping an internal record of the incident
(**58%** of businesses and **69%** of charities)

Assessing the scale and impact of the incident
(**56%** of businesses and **63%** of charities)

Debriefing to record lessons learnt from the incident
(**54%** of businesses and **62%** of charities)

Informing cyber-insurance providers, among those with insurance
(**52%** of businesses and **56%** of charities)

Informing a regulator of the incident when required
(**47%** of businesses and **55%** of charities)

Attempting to identify the source of the incident
(**45%** of businesses and **46%** of charities)

Using a National Cyber Security Centre (NCSC)-approved incident response company
(**15%** of businesses and **11%** of charities)

In response to experiencing a breach, **62%** of businesses and **67%** of charities took steps to protect their organisations from future attacks. These efforts included:

Enhanced staff training or communications

Technical changes (such as updated antivirus software)

Governance changes (such as increased monitoring)

However, 36% of businesses and 31% of charities took no action at all.

Approaching Cyber-security

This section provides information on the actions organisations have taken to bolster their cyber-security efforts in the last 12 months, including common technical controls, board engagement efforts and cyber-hygiene measures.

Cyber-security Controls and Policies

The most common technical controls organisations implemented to bolster their cyber-security included:

1. **Using up-to-date malware protection** (**77%** of businesses and **64%** of charities)
2. **Enforcing a password policy that ensures users select strong passwords** (**73%** of businesses and **57%** of charities)
3. **Using firewalls that cover the network and individual devices** (**72%** of businesses and **49%** of charities)
4. **Backing up data securely via a cloud service** (**71%** of businesses and **58%** of charities)
5. **Restricting IT admin and access rights for specific users** (**68%** of businesses and **68%** of charities)

The least common technical controls organisations implemented to bolster their cyber-security included:

1. **Monitoring of user activity** (**30%** of businesses and **31%** of charities)
2. **A VPN for staff connecting remotely** (**31%** of businesses and **20%** of charities)
3. **A software security updates policy** (**32%** of businesses and **21%** of charities)
4. **Separate wi-fi networks for staff and visitors** (**33%** of businesses and **27%** of charities)
5. **Two-factor authentication** (**40%** of businesses and **35%** of charities)

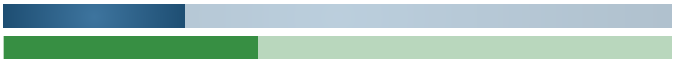
36% of businesses and **35%** of charities had a formal policy or policies covering cyber-security risks. Of these:

47% of businesses and **35%** of charities reviewed their cyber-security policies within the last six months.

13% of businesses and **21%** of charities have not created, updated or reviewed their policies in over a year.

Board Engagement

Cyber-security remains a high priority for **72%** of businesses and **68%** of charities.



27% of businesses have a board member responsible for cyber-security (this has gradually declined since 2021, when it was **38%**).

Approaching Cyber-security (cont.)

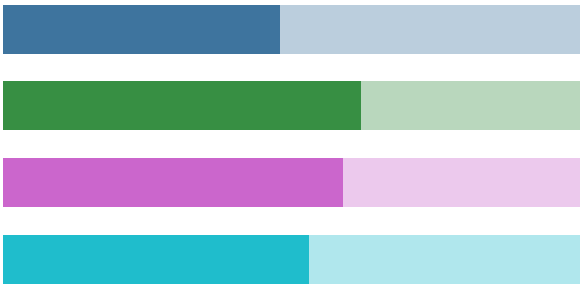
Recognising Supplier Risks

Only **14%** of businesses and **9%** of charities formally reviewed the potential cyber-security risks presented by their immediate supply chains, and fewer included their wider supply chains.

Larger organisations fared better; nearly half of large businesses (**45%**) reviewed the cyber-security risks posed by their immediate suppliers compared to **11%** of micro-business and **21%** of small businesses.

Cyber-hygiene Measures

Small businesses increased several cyber-hygiene measures:



48% undertook cyber-security risk assessments (up from 41% in 2024).

62% had cyber-insurance in place, either from a specific policy or as cover from a wider insurance policy (up from 49% in 2024).

59% had a formal policy covering cyber-security risks (up from 51% in 2024).

53% had a business continuity plan that covered cyber-security (up from 44% in 2024).

High-income charities saw a decline in several cyber-hygiene measures:

75% conducted activities to identify cyber-threats (down from 86% in 2024).

39% had a formal cyber-security strategy in place (down from 47% in 2024).

21% reviewed the cyber-risks posed by their immediate suppliers (down from 36% in 2024), and only **6%** reviewed their wider supply chains (down from 15% in 2024).

Government Initiatives, Insurance Trends and Risk Identification

This section provides information on cyber-insurance trends, actions taken to identify cyber-security risks and awareness of government cyber-initiatives.

Understanding Government Initiatives

Only **24%** of businesses and **26%** of charities were aware of the NCSC Cyber Aware campaign (awareness has steadily declined since 2021, when 34% of businesses and 38% of charities were aware of it.)

Just **12%** of businesses and **15%** of charities were aware of the government's "10 Steps to Cyber Security" and Cyber Essentials scheme.

Cyber-insurance

45% of businesses and **34%** of charities were insured against cyber-risks in some way.

38% of businesses and **29%** of charities had cyber-security cover as part of a wider insurance policy.

Only **7%** of businesses and **5%** of charities had a specific cyber-insurance policy in place.

Larger businesses (**18%** of medium businesses and **27%** of large businesses) and high-income charities (**23%**) were more likely to have a specific cyber-insurance policy in place.

Identifying Cyber-security

49% of businesses and **42%** of charities took action to identify cyber-security risks in the past 12 months. Top actions included:

Using specific tools designed for security monitoring (**30%** of businesses and **24%** of charities)

Conducting risk assessments related to cyber-security threats (**29%** of businesses and **29%** of charities)

Testing staff using methods such as mock phishing exercises (**18%** of businesses and **14%** of charities)

Carrying out a cyber-security vulnerability audit (**15%** of businesses and **13%** of charities)

Penetration testing (**12%** of businesses and **9%** of charities)

Investing in threat intelligence (**9%** of businesses and **6%** of charities)

Large organisations were more likely to carry out these actions; **92%** of large businesses, **84%** of medium businesses and **75%** of high-income charities carried out at least one identification activity.

The Importance of Cyber-security

Top Reasons to Invest in Cyber-security

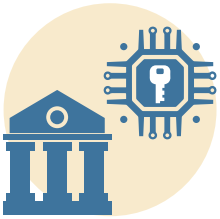
Protect customer and consumer data.

Protect trade secrets, intellectual property and other assets.

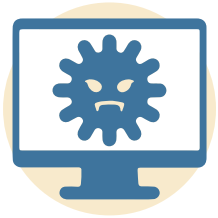
Prevent fraud or theft.

Promote business continuity.

Protect the organisation's reputation.



Comply with data protection laws.



Protect against computer viruses.

Protect remote employees.

Glossary of Organisation Sizes

Organisation sizes

The following are definitions used by the government to describe organisations of various sizes.

Micro-business	Businesses with one to nine 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
Low-income charity	Charities with an income of less than £100,000
High-income charity	Charities with an income of £500,000 or more

---

Data Sources and Reliability

This year's data was gleaned from the responses of UK businesses over 12 months. Main survey interviews and qualitative follow-up interviews took place between August and December 2024.

Please note that the data wasn't based on the entire population of UK businesses or charities but rather on weighted samples. As such, percentage results are subject to margins of error. Visit the government website for more information.