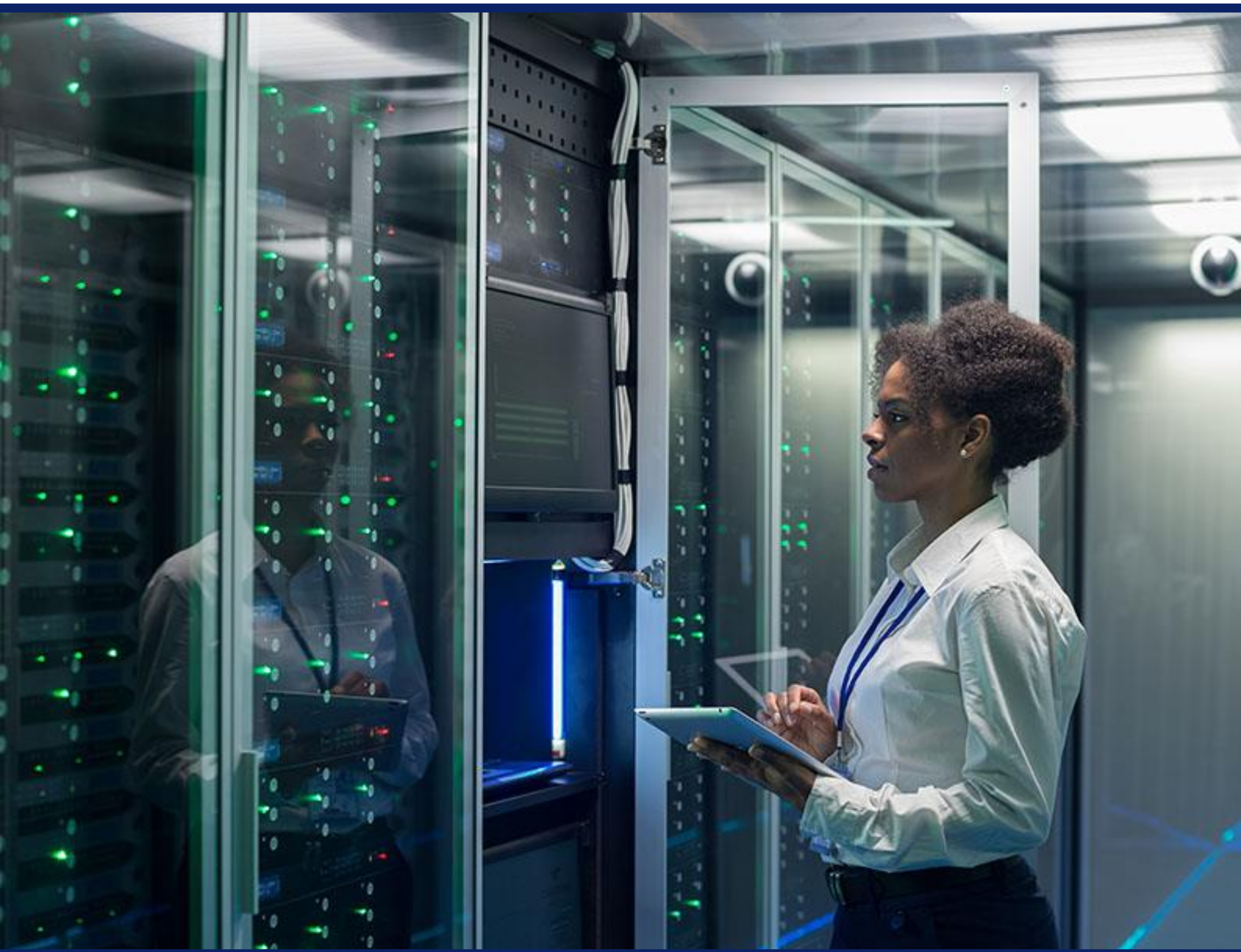
trowers & hamlins

trowers.com

Cyber security breaches survey 2025

Insights from breaches to best practice



May 2025

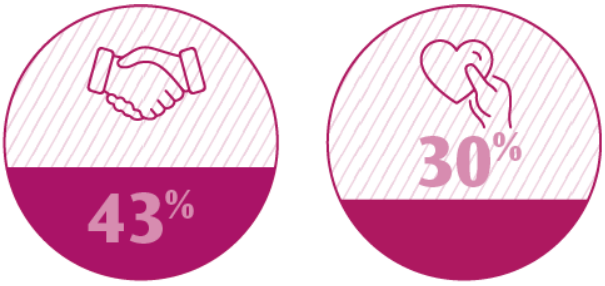
Cyber Security Breaches Survey 2025

On 10 April 2025, the Department for Science, Innovation & Technology (the 'DSIT') published its annual Cyber Security Breaches Survey (the 'Survey'). The Survey delves into the policies, processes and approach to cyber security by UK businesses and charities and highlights trends in cyber security awareness, approaches to risk management, and the prevalence and impact of breaches, incident response, and the evolving threat of cybercrime.

Cybersecurity incidents

In the 12 months prior to the Survey, 43% of business and 30% of charities reported experiencing some kind of cyber security breach or attack. This is believed to affect 612,000 businesses and 61,000 charities each year.

The most common type of attack was phishing, affecting 85% of businesses and 86% of charities. Phishing attacks cited as disruptive due to their volume, and the need for investigation and staff training. However, organisations had a growing awareness that increasingly sophisticated methods, such as AI impersonation, were becoming mainstream.

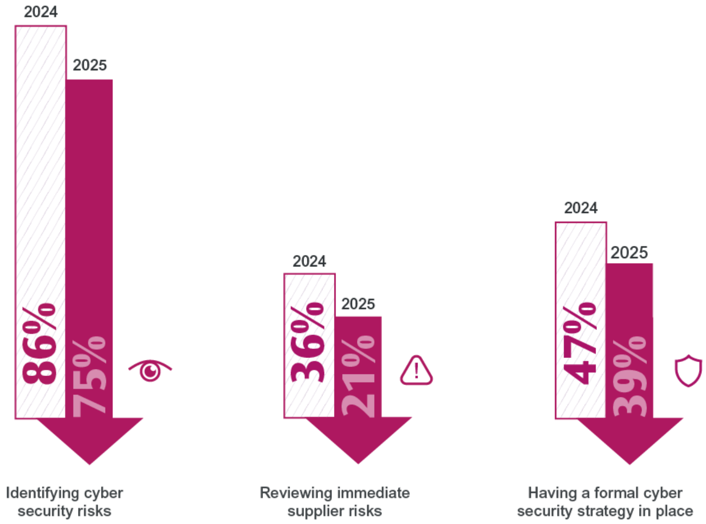


Businesses and charities reporting a cyber security breach in the last 12 months

Current protections in place by organisations

Cyber hygiene measures

An increasing number of small businesses showed an uptake of cyber hygiene measures, such as cyber security risk assessments (48%, an increase from 41% in 2024), cyber insurance (62% up from 49% in 2024), formal cyber security policies covering cyber security risks (59% up from 51% in 2024), and business continuity plans that address cyber security (53% up from 44% in 2024).

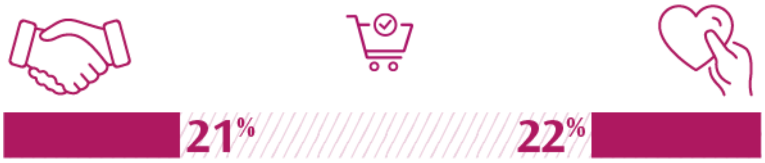


However, despite the continued prevalence of cybersecurity attacks and breaches, high-income charities show a reduction in activities in several key areas compared to 2024 (likely due to budget constraints) such as: identifying cyber security risks (75% down from 86% in 2024), reviewing immediate supplier risks (21% down from 36% in 2024), and having a formal cyber security strategy in place (39% down from 47% in 2024).

Risk management

Further, the Survey asked businesses and charities about their risk management procedures. The results are that 31% of businesses were undertaking cyber security risk assessments which remained in line with the previous year, which was at 29%. However, a much largest number of small businesses, compared to the previous year were carrying out risk assessments covering cyber security (48% in 2025, 41% in 2024). Of concern, when reviewing risks, only 14% of businesses and 9% of charities reviewed the risks posed by immediate suppliers and only 7% of businesses and 4% of charities reviewed the risks posed by their wider supply chain.

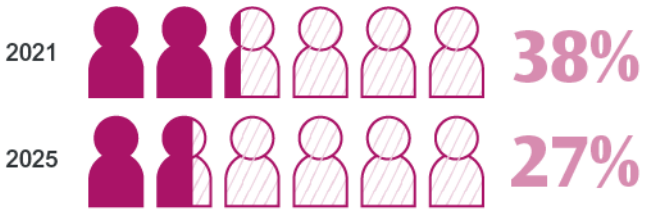
A new question for 2025 added to the theme of managing risk, by asking about the role that cyber security considerations played when purchasing new software. Around 21% of businesses and 22% of charities considered cyber security to a "large extent" when purchasing software. For the majority of businesses and charities however, this was not a major concern and for significant minority (being 14% of businesses and 16% of charities) it was not a consideration at all.



Businesses and charities that considered cyber security to a "large extent" when purchasing software.

Governance and board engagement

In terms of levels of board engagement and corporate governance approaches towards cyber security, although cyber security has remained a high priority for the majority of business, in line with previous years, there has been a steady decline among business since 2021 whereby only 27% of businesses have a board member with responsibility for cyber security, compared to 38% in 2021.



Businesses with a board member with a responsibility for cyber security

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

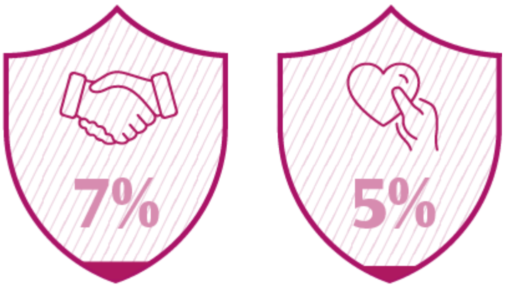
Key takeaways from the Survey

Whilst it is clear that cyber security remains a high risk area for businesses and charities alike, in line with previous years there are further steps that organisations can take to have more robust procedures in place and to prevent against potential attacks, or at the very least, reduce an attack's financial impact and/or business interruption.

We set out below several steps that an organisation can take to enhance their cybersecurity:

- **Enhance training and awareness:** the Survey found that tackling phishing would likely be key in helping to guard against some of the most disruptive and costly impacts associated with cyber breaches and attacks. As such, robust defences and effective staff training continue to be crucial in the battle against phishing attacks. Generally, staff training was cited as the most common preventative measure adopting by organisations following a breach or attack, highlighting the importance of ongoing education and awareness raising.

  Consider insurance options: currently 45% of businesses and 34% of charities are insured against cyber security risks in some way, however this is mostly as part of a wider policy. Only 7% of businesses and 5% of charities had specific cyber security insurance policy. It is also worth noting that 20% of businesses and 19% of charities did not know if they had any form of cyber security insurance. It is crucial for organisations to be aware of the insurance position and options and investigate those thoroughly.



Businesses and charities that have a specific cyber security insurance policy.

- **Adopt more advanced technical controls:** while there has been an increase in small businesses adopting cyber hygiene practices, large organisations already benefit from formal strategies and established processes and although they have implemented basic technical controls, there remains room for improvement by adopting technical controls like two-factor authentication and VPNs.

We regularly advise clients on how to mitigate risk and prioritise cyber planning for their business. We have the knowledge, understanding and solutions regardless of the client's market or size to be able to work with clients and provide them with the tools required to protect against cyber attacks or breaches.

Combining the legal excellence of Trowers cyber team and award-winning cyber experts, CyberQ, CyberSecure 360 offers legal and technical cybersecurity advice tailored to clients' requirements – from assessing compliance with cyber policies, undertaking risk assessments through penetration testing and incident response planning to providing training and playing out war-room scenarios in real time.

For more information or to discuss your cyber and fraud prevention needs please contact our specialist CyberSecure 360 team: cybersecure360@trowers.com

Our team

Charlotte Clayson

Partner

Dispute Resolution and Litigation

☎ +44 (0)20 7423 8087

✉ cclayson@trowers.com

Helen Briant

Partner

Dispute Resolution and Litigation

☎ +44 (0)121 214 8867

✉ hbriant@trowers.com

Sanchita Agrawal

Associate

Dispute Resolution and Litigation

☎ +44 (0)20 7423 8312

✉ sagrawal@trowers.com

Joseph Hannify

Associate

Dispute Resolution and Litigation

☎ +44 (0)20 7423 8425

✉ jhannify@trowers.com