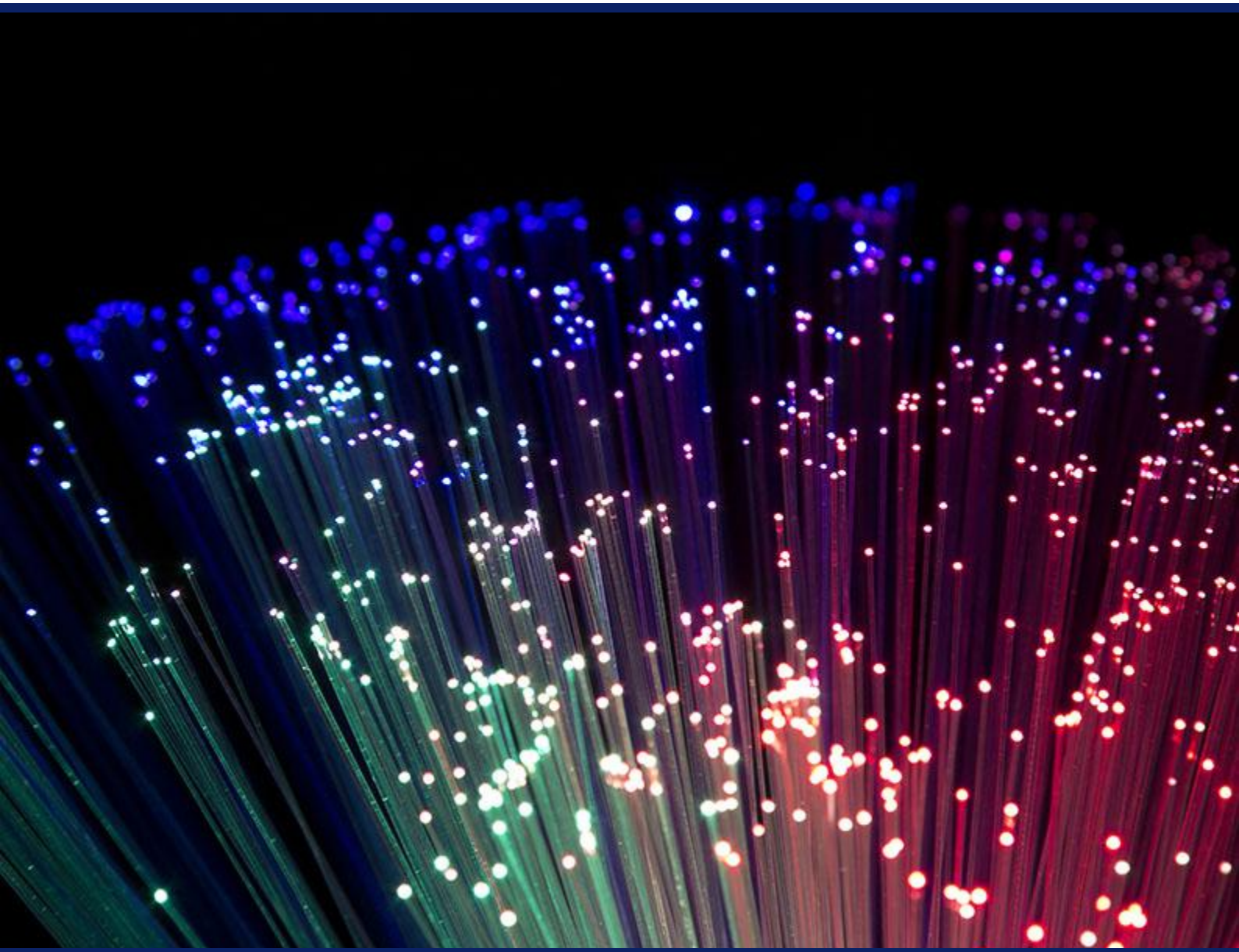
trowers & hamlins

trowers.com

Cyber Security Breaches Survey 2026

Insights from breaches to best practice



June 2026

Cyber Security Breaches Survey 2026

How well is your organisation really prepared for a cyber attack? The UK Government's annual Cyber Security Breaches Survey – commissioned by the Department for Science, Innovation and Technology and the Home Office – offers one of the most comprehensive answers to that question.

Drawing on quantitative and qualitative research carried out between August and December 2025, the 2025/2026 edition (published 30 April 2026) explores organisational policies and processes, the prevalence and impact of breaches, incident response and cyber crime.

The headline message is one of stabilisation rather than improvement: reported breach levels have held steady following a notable decline the previous year, but persistent weaknesses in governance, planning and supply chain oversight mean that many organisations remain more exposed than they need to be.

Over the last 12 months we have also seen how the exploitation of a single vulnerability can debilitate even the largest of companies, wipe millions from the bottom line, and have ripple effects throughout an entire industry, and the wider economy. In this report, we look at the key findings and what they mean in practice for your own cyber resilience.

How Widespread Is the Problem?

Just over four in ten businesses (43%) and around three in ten charities (28%) reported experiencing a cyber security breach or attack in the preceding 12 months, equating to approximately 612,000 businesses and 57,000 charities.

Just over four in ten businesses (43%) and around three in ten charities (28%) reported experiencing a cyber security breach or attack in the preceding 12 months.

For businesses, this figure is unchanged from the previous year, having already fallen from 50% in 2023/2024 to 43% in 2024/2025. For charities, prevalence also remained broadly in line with last year, although high-income charities saw a more notable decline, falling from 66% in 2023/2024 to 57% in 2025/2026.

Size remains a significant factor: medium (65%) and large (69%) businesses were considerably more likely to report a breach than micro (42%) or small (46%) businesses. The survey can only capture incidents that organisations identified and were willing to report, so the true scale may well be underestimated.

The Nature of the Threat: What Organisations Are Facing

Phishing continues to dominate. It remained the most prevalent type of breach or attack (38% of businesses; 25% of charities) and was most commonly identified as the most disruptive incident (69% of affected businesses and charities alike).

Phishing remained the most prevalent type of breach or attack (38% of businesses; 25% of charities)

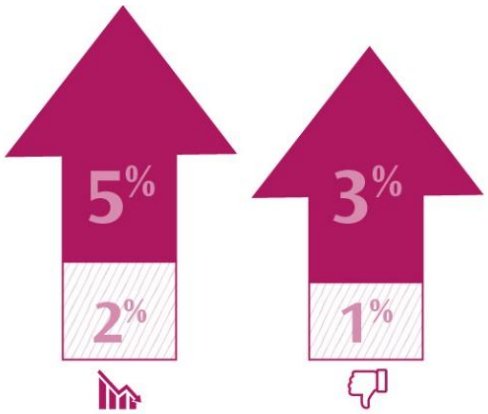
The proportion of organisations experiencing phishing as their only type of attack is increasing: among those that experienced any breach, "phishing only" incidents rose from 45% to 51% for businesses and from 46% to 57% for charities. Qualitative interviews suggested that respondents perceived phishing attacks as growing in sophistication, making them harder for employees to identify.

Some threat types declined. Reports of ransomware attacks among businesses fell to 1% (from 3% in each of the two preceding years), and impersonation attacks fell to 12% (from 17% in 2023/2024). Among charities, impersonation fell to 7% (from 11% in 2024/2025) and account or device takeovers declined from 3% to 1%.

What Is the Impact of Breaches?

Among those that identified an incident, 19% of businesses and 11% of charities reported at least one negative outcome, with temporary loss of access to files or networks (8% of businesses; 3% of charities) and disruption to websites or online services (6% businesses; 4% charities) being the most commonly cited.

More broadly, 30% of businesses and 26% of charities reported being affected in at least one of the ways measured, such as requiring new controls or absorbing significant additional staff time. Some categories increased year-on-year, including loss of revenue or share value (from 2% to 5% of affected businesses) and reputational damage (from 1% to 3%).

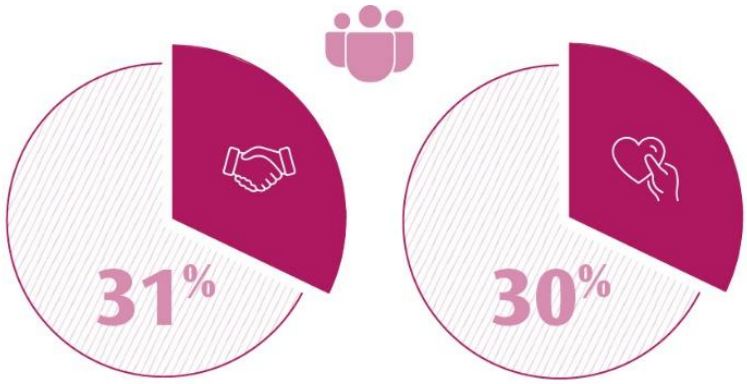


Some categories increased year-on-year, including loss of revenue or share value (from 2% to 5% of affected businesses) and reputational damage (from 1% to 3%).

Governance, Risk Management and Oversight

The survey also examines the frameworks organisations have in place to manage cyber risk on an ongoing basis.

Cyber security is viewed as a high priority by senior management in 72% of businesses and 60% of charities. The latter figure represents a significant decline from 68% in 2024/2025, which is a concern given that charities frequently hold sensitive personal data and may have limited resources for recovery.



Board-level responsibility for cyber security is formally assigned in 31% of businesses and 30% of charities

Board-level responsibility for cyber security is formally assigned in 31% of businesses and 30% of charities, rising to 68% among large businesses. For businesses, the 31% figure represents an increase from 27% in 2024/2025, reversing a longer-term declining trend. This is encouraging, though overall board engagement continues to leave room for improvement.

Around a third of businesses (30%) and charities (27%) conducted a cyber security risk assessment in the last year. Supply chain risk management remains a particular weakness: only 15% of businesses and 9% of charities reviewed the risks posed by their immediate suppliers, while scrutiny of the wider supply chain was even less common (6% of businesses; 4% of charities). At a time when supply chain vulnerabilities are an increasingly recognised attack vector, these figures suggest many organisations remain exposed.

Only 15% of businesses and 9% of charities reviewed the risks posed by their immediate suppliers.

Technical Controls and Cyber Hygiene

The most widely used controls among businesses included up-to-date malware protection (81%), cloud backups (74%), network firewalls (74%), password policies (74%) and restricted administrative rights (73%). Among charities, figures were lower across the board, ranging from 65% (restricted admin rights) to 45% (firewalls).

Adoption of other controls was considerably lower. Multi-factor authentication was in place at 47% of businesses and 38% of charities, VPNs at 36% and 17% respectively, and user monitoring at 33% and 28%.

Small businesses showed a reversal in several cyber hygiene measures, including declines in risk assessments, formal cyber security policies and business continuity plans. This is particularly notable given that smaller businesses typically have less capacity to absorb the disruption of a significant incident.

Insurance and Incident Response

Almost half of businesses (47%) and just over a third of charities (35%) reported having some form of cyber insurance, meaning that the majority of charities and a significant proportion of businesses would face an incident without dedicated insurance protection.

Only 25% of businesses and 19% of charities had a formal incident response plan.

Only 25% of businesses and 19% of charities had a formal incident response plan, rising to 57% of medium businesses, 76% of large businesses and 49% of high-income charities. For the majority of the 43% of businesses that experienced a breach in the past year, there was no pre-defined plan to guide the response.

Where breaches occurred, internal reporting was most common: 81% of affected businesses and 84% of affected charities informed directors or trustees. External reporting was less frequent, with 40% of businesses and 36% of charities reporting their most disruptive breach outside the organisation.

Following an incident, 61% of businesses and 57% of charities took some action to prevent future occurrences, most commonly people and training-related changes (31% of businesses; 37% of charities).

Cyber Crime

An estimated 19% of businesses and 14% of charities were victims of at least one cyber crime in the past year, equating to approximately 267,000 businesses and 28,000 charities. Prevalence was broadly stable compared with the previous two years.

Phishing dominated, affecting 93% of businesses and charities that experienced any cyber crime (18% of all businesses; 13% of all charities).

Cyber-facilitated fraud affected 3% of businesses and 1% of charities (around 43,000 businesses and 3,000 charities), stable compared with the previous year.

What Should Organisations Take Away from This?

The survey does not point to a dramatic escalation in attacks, but nor does it suggest that organisations are becoming materially more resilient.

- **The continuing rise in phishing-only attacks** and their growing sophistication suggests that technical controls and staff awareness training need to keep pace with evolving tactics rather than simply maintaining existing measures.

- **The low levels of supply chain scrutiny are a significant gap.** As regulators and insurers increasingly focus on supply chain risk, organisations that have not yet reviewed their suppliers' cyber security practices should treat this as a key priority.

- **The gap in incident response planning** between large organisations and the rest of the market remains substantial. A formal plan need not be complex, but having one in place, tested and understood, can make a material difference to impact and subsequent recovery following an incident.

- **The decline in senior management prioritisation of cyber security** among charities is worth monitoring. Charitable organisations often handle significant volumes of sensitive personal data, and a weakening of governance focus carries risk both to data subjects and to the charity's own reputation and operational continuity. The Government's Cyber Governance Code of Practice provides a useful framework for boards and senior leaders seeking to strengthen their oversight of cyber risk. You can read our own analysis of the Code and its practical implications here.

If any of the themes raised here resonate with your own organisation's experience, or if you would like help reviewing your cyber security arrangements, incident response plans or supply chain oversight, get in touch with our Cyber 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

Joseph Hannify
Associate
Dispute Resolution and Litigation
+44 (0)20 7423 8425
jhannify@trowers.com