Cyber security for small organisations

The 2026 figures

Cyber security for small organisations: the 2026 figures

The government's survey counts only the breaches organisations noticed and were willing to report. Even so, two gaps that now fail a Cyber Essentials assessment automatically, missing multi-factor authentication and late security updates, sit among the least common controls it records.

Written for owners, operations and finance leads, and trustees of organisations with fewer than 250 staff, including charities, deciding how much attention security needs this year.

What the survey counts

The Cyber Security Breaches Survey, published by the Department for Science, Innovation and Technology and the Home Office on 30 April 2026, questioned 2,112 UK businesses and 1,085 UK registered charities between August and December 2025, weighted to represent both. Sole traders, and businesses with no IT capacity or online presence, are outside it. It counts only the breaches organisations were able to identify and willing to report, and says its findings may therefore underestimate the full extent.

43%

of businesses reported a breach or attack in the last 12 months (28% of charities). Only those identified and reported count.

Breaches survey 2025/2026

38%

of businesses experienced phishing in that period, by far the most common type (25% of charities).

Breaches survey 2025/2026

15%

of businesses said they reviewed the risks posed by their immediate suppliers (9% of charities).

Breaches survey 2025/2026

The common assumption is that a small organisation is too small to be a target. The figures say otherwise: 42 per cent of micro businesses (one to nine employees) and 46 per cent of small businesses (ten to 49) reported a breach or attack, against 65 per cent of medium and 69 per cent of large ones. The survey itself says the lower rates may reflect poorer identification and reporting in smaller organisations, which may have less sophisticated monitoring. A lower rate may be a lower count rather than a lower risk. Preparation falls away with size much faster than reported breaches do: a formal incident response plan was held by 76 per cent of large businesses but by 21 per cent of micro businesses.

The controls gap

Cyber Essentials, which the NCSC calls the minimum standard the government recommends for organisations of all sizes, kept its five controls in April 2026 and tightened its marking. For assessment accounts created after 26 April, two gaps now fail an assessment automatically: a cloud service without multi-factor authentication where it is available, and a high-risk or critical security update not installed within 14 days of release. Accounts created before that date have six months to certify under the previous version. The survey's nearest measures are among the least common controls it records: 47 per cent of businesses have any requirement for two-factor authentication (43 per cent of micro businesses), and 34 per cent have a policy of applying security updates within 14 days.

Measure: businesses, then charities	What it means in practice
Board or trustee responsible: 31% and 30%	Firms without a formal board may lower the first figure, the survey warns. Every registered charity has trustees.
Aware of Cyber Essentials: 17% and 16%. Report adhering to it: 5% and 3%	18 per cent of businesses did not know whether they adhered to it, Cyber Essentials Plus or ISO 27001. Yet 24 per cent of businesses report controls in all five of its areas, on a survey proxy that leaves out two-factor authentication.

Ten questions, one for each of the 10 Steps

The NCSC writes its 10 Steps for medium to large organisations, points smaller ones to its Cyber Action Toolkit, and says the principles apply to all. The survey maps a measure to each step, imperfectly by its own account. The figures below are for businesses.

- ☐ Has anyone assessed the organisation's cyber risk, and who at the top owns it?
  Risk management. 30% did a cyber risk assessment in the last 12 months.
- ☐ Would staff recognise a convincing phishing email, and know where to report it?
  Engagement and training. 19% ran staff training or awareness activity in the past year.
- ☐ Is there a list of the devices, accounts, cloud services and data that matter most?
  Asset management. 29% keep a list of critical assets. Cyber Essentials scope cannot exclude cloud services.
- ☐ Have default passwords been changed, and unused accounts and software removed, on every device?
  Architecture and configuration. Required by Cyber Essentials. The survey's measure is looser, any three of eight listed controls: 81%.
- ☐ Are high-risk and critical updates installed within 14 days of release, on everything?
  Vulnerability management. 34% have a 14-day update policy.
- ☐ Does every cloud service ask for a second factor, and does access end when someone leaves?
  Identity and access management. 47% have any two-factor requirement. Cyber Essentials v3.3 counts FIDO2 passkeys as multi-factor.
- ☐ When was a backup last restored, and was what came back checked?
  Data security. 88% keep backups. Cyber Essentials does not require them; the NCSC highly recommends them.
- ☐ If an account had been misused last month, would anything show it?
  Logging and monitoring. 48% use security monitoring tools or monitor user activity.

- [ ] Is there a written incident response plan, and has the leadership rehearsed it?
  Incident management. 25% have a formal plan; the survey's 44 interviews found plans largely untested or incomplete. The NCSC's Exercise in a Box is free.

- [ ] Which suppliers hold the organisation's data or reach its systems, and what was asked of them?
  Supply chain security. 16% monitor risks from suppliers or the wider supply chain.

Where to go

For	Where it is listed, and what the listing says
Cyber Essentials	IASME, the NCSC's delivery partner, lists the bodies it licenses in Find a Certification Body. Prices depend on organisation size, starting at £320 plus VAT. NCSC-assured Cyber Advisors help small and medium sized businesses put the five controls in place.
A live incident	The NCSC recommends an assured Cyber Incident Response provider to every UK organisation, charities included. Its service at gov.uk/report-cyber does not share reports with the ICO, so a personal data breach may need its own report.
A penetration test	Cyber Essentials does not cover bespoke parts of web applications. The NCSC says testing can usefully be applied to in-house systems, should be done by qualified and experienced staff only, and validates only against known issues on the day. Its CHECK scheme is not needed outside the public sector.

Sources

DSIT and Home Office, Cyber security breaches survey 2025/2026, 30 April 2026: summary, methodology, chapters 2 to 5, Figures 3.1, 3.2 and 3.6, Table 3.1, qualitative findings on incident response, and the footnote defining the five Cyber Essentials areas.

NCSC, Cyber Essentials: Requirements for IT Infrastructure v3.3, April 2026: Backing up your data, Scope (cloud services, software development), Secure Configuration, Security Update Management, User Access Control and Passwordless authentication.

IASME, the NCSC's Cyber Essentials Delivery Partner, Important update: changes to Cyber Essentials for April 2026, 12 February 2026: marking criteria, questions A6.4 and A6.5, dates and transition.

NCSC, Cyber Essentials overview: status of the scheme, delivery partner, prices, Cyber Advisors.

NCSC, 10 Steps to Cyber Security, published 11 May 2021: who the guidance is for.

NCSC, Exercise in a Box: overview.

NCSC, Cyber Incident Response scheme: introduction.

GOV.UK and NCSC, Where to report a cyber incident, published 13 May 2022 (gov.uk/report-cyber redirects here).

IASME, Find a Certification Body.

NCSC, CHECK penetration testing: information for buyers.

NCSC, Penetration testing guidance, published 8 August 2017, reviewed 10 January 2022: what sort of system should be tested, and using penetration testing effectively.

What this brief is not

This brief is not a Cyber Essentials assessment, a certificate or legal advice, and answering its ten questions certifies nothing. We do not certify, assess, test or monitor anything. The survey describes businesses and charities in aggregate, not any one organisation. Sources last checked 19 September 2026.

Theo Coleman
Chief Technology Officer, BespokeWorks. June 2026