

The 7% Problem: stat pack

Companion to the TrustLayer Pulse Check 2026. Every figure in the report, with its source, its publication date and the working behind it.

What this is

We published *The 7% Problem* without a form in front of it, and this is the same principle applied to the data. If you want to use any of these figures in a board paper, a budget case or your own writing, everything you need to check them is here.

Two of the numbers in the report are ours rather than the government's. Those are set out in full below, including the arithmetic, so you can decide for yourself whether you find them persuasive.

The sources

1 Cyber Security Breaches Survey 2025/2026

Department for Science, Innovation and Technology, with the Home Office. Published 30 April 2026. Fieldwork carried out by Ipsos between August and December 2025, covering 2,112 UK businesses, weighted to be representative of the UK business population. These are official statistics.

gov.uk/government/statistics/cyber-security-breaches-survey-20252026

2 The hidden risks of shadow AI

National Cyber Security Centre. Published 7 September 2026.

ncsc.gov.uk/blogs/the-hidden-risks-of-shadow-ai

3 TrustLayer 2025 UK Cyber Resilience Report

Our own fieldwork, conducted with 3Gem between 8 and 21 January 2024, covering 280 IT leaders in UK SMBs.

The threat picture

All from source 1.

FIGURE	WHAT IT MEASURES
43%	of businesses experienced a cyber breach or attack in the last 12 months. Unchanged year on year.
38%	experienced phishing. The most prevalent attack type by a wide margin.
69%	of breached businesses named phishing the most disruptive attack they faced.
12%	experienced impersonation attacks, down from 17% in 2023.
1%	experienced ransomware, down from 3%.

On the qualitative side, security teams told the researchers that phishing had become easier for attackers to commit, and that the grammatical errors which once made a malicious email obvious were becoming less common. This is perception data from interviews rather than measurement, and the report treats it as such.

AI adoption and AI controls

All from source 1.

FIGURE	WHAT IT MEASURES
31%	of UK businesses are using AI, in the process of adopting it, or actively considering it.
21%	have adopted some AI tools. A further 4% are in the process, and 6% are actively considering.
39%	AI adoption among medium businesses.
45%	AI adoption among large businesses.
24%	of the 31% above have security practices in place to manage AI risk.
38%	of that group plan to put practices in place within 12 months.
31%	of that group have no plans to do so at all.

Referenced in source 2: **71%** of UK employees have used AI tools that their employer has not approved.

An important note on that figure. It originates in Microsoft and Censuswide research on UK employees, referenced by the NCSC, and should be attributed to that research rather than to the NCSC. It counts individual employees, not businesses, so it is not directly comparable with the DSIT figures above and should not be combined with them into a single statistic. We have been careful about this throughout and would ask anyone quoting it to be the same.

The two figures that are ours

Both are arithmetic on the DSIT percentages above. Neither appears in the DSIT release, because DSIT reports the two components separately.

7%

Roughly 7% of UK businesses have AI in use or planned and controls around it.

31% are using, adopting or considering AI. Of that group, 24% have security practices for AI risk.

$$0.31 \times 0.24 = 0.0744$$

so approximately 7% of the business population, or about one in fourteen.

10%

Roughly 10% are adopting AI with no plans to secure it.

31% are using, adopting or considering AI. Of that group, 31% have no plans to put practices in place.

$$0.31 \times 0.31 = 0.0961$$

so approximately 10%.

Both are rounded, and both are derived from separately reported percentages rather than a single cross-tabulation, so treat them as close estimates rather than precise counts. If you quote them, the honest framing is that DSIT publishes both components and TrustLayer multiplied them.

The controls that are not keeping up

All from source 1. Where the survey publishes a breakdown by business size, it is shown. Where it publishes only an overall figure, the other columns are left blank rather than estimated.

CONTROL	ALL	MICRO	SMALL	MEDIUM	LARGE
Staff training or awareness in last 12 months	19%	14%	33%	54%	84%
Test staff with mock phishing	22%				
Agreed process for reporting suspicious emails	58%				
Any two-factor authentication	47%				
Monitoring of user activity	33%				
Policy to apply security updates within 14 days	34%				
Formal incident response plan	25%	21%		57%	76%
Cyber risk assessment carried out	30%		41%	62%	72%
Formal cyber security policy	36%	31%	52%	75%	89%
Review immediate supplier risk	15%	12%	22%	30%	48%

Staff training has been flat at 19% for two consecutive years.

Small businesses went backwards

All from source 1. Each of these reversed a gain made the previous year.

MEASURE	PREVIOUS	LATEST
Cyber risk assessments	48%	41%
Formal security policies	59%	52%
Business continuity plans covering cyber	53%	44%

The figure from our own research

From source 3: **65%** of the UK organisations we surveyed allowed unrestricted app downloads with no visibility into what staff were using.

The fieldwork for that was January 2024, which is why the report uses it as historical context rather than as a current reading. The point it makes is that the visibility gap existed before AI became a workplace tool.

Using these figures

Everything here is either public or ours, and you are welcome to use it. We would ask three things:

-
- 1 Attribute the DSIT figures to the Cyber Security Breaches Survey 2025/2026 rather than to TrustLayer. They are not ours.
 - 2 Attribute the 71% to Microsoft and Censuswide research referenced by the NCSC, not to the NCSC itself, and do not set it alongside business-level figures as if they measured the same thing.
 - 3 If you use the 7% or 10% figures, say that they are derived from two separately reported DSIT figures. We would rather they were quoted accurately than quoted often.
-

Questions

If something here does not add up, or you want a cut of the data that is not shown, email sales@trustlayer.co.uk and it will reach someone who can answer.

If you want to know where your own organisation sits rather than where the average one does, the AI exposure check takes about two minutes at ai.trustlayer.co.uk. Nothing you click leaves your browser.

TrustLayer Pulse Check 2026. Published October 2026.