A 2026 REPORT FOR PROFESSIONAL FIRMS IN LONDON, THE SOUTH EAST AND THE EAST OF ENGLAND

TRUSTED OR TARGETED?

What your clients check before they hire you, how criminals use your name to divert your fees, and what happens when client data gets out.



November 2026

AT A GLANCE

Six numbers for any firm that **sells its expertise**

Who this report is for

You may not call yourself a consultancy. You might be a practice, a studio, a partnership or an institute. What you have in common with the other firms in this report is that you sell expertise, bid for the work, invoice for it and look after your clients' information while you do it.

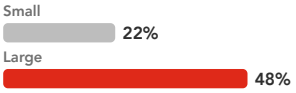
Architects · Engineers · Surveyors · Planners · Management consultants · HR and people advisers · Researchers · Economists and policy teams · Risk and compliance advisers · Environmental consultants · Think tanks

59%



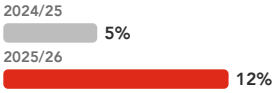
of the 420 professional firms we checked have email that a criminal can fake in their name.

48%



of large businesses check their suppliers' cyber security. Only 22% of small ones do.

12%



of small businesses hold Cyber Essentials, up from 5% a year earlier.

16,034



data breach reports to the ICO from all sectors in the year to September 2026, up 24%.

46%



of small businesses had a cyber breach or attack in the last 12 months.

£41.3m



lost to invoice and mandate fraud in 2025, 68% of it from business accounts.

01
Trusted
What your clients and public buyers check before they hire you.
PAGE 3

02
Targeted
How criminals use your name to divert the fees you invoice.
PAGE 6

03
Targeted
What happens when client data gets out, and how often it does.
PAGE 10

04
Trusted, not targeted
Nine things to do, in the order we'd do them.
PAGE 12

SOURCES

59%. Public DNS records of 420 firms read by AIS Technology on 12 Nov 2026.

48%, 22%, 12%, 46%. DSIT, Cyber Security Breaches Survey 2025/26, 30 April 2026.

16,034. ICO data security incident trends, Q4 2025 to Q3 2026, all sectors, one record per report. Analysis by AIS Technology.

£41.3m. UK Finance, Annual Fraud Report 2026.



PART ONE

TRUSTED: WHAT CLIENTS CHECK **BEFORE THEY HIRE YOU**

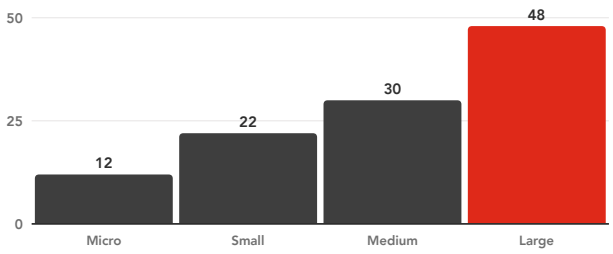
Bigger clients and public buyers want proof that a supplier can be trusted with their information. For a firm that wins work through bids and frameworks, that proof can be part of the price of entry.

PART ONE · TRUSTED

Your biggest clients are the ones checking

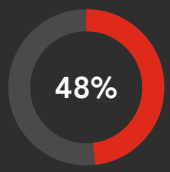
The government's 2026 survey found that the bigger the business, the more likely it is to review the cyber risk its suppliers pose. Nearly half of large businesses now do it. Those are the clients a growing professional firm most wants to win.

Businesses that review the cyber risks posed by their immediate suppliers



By size of business. Large shown in red.

YOUR BIGGER CLIENTS



of large businesses review the cyber risk posed by their suppliers, against 22% of small businesses.

Public buyers have asked since 2014

Central government has required suppliers bidding for certain contracts to hold Cyber Essentials, or show equivalent controls, since 2014. The current policy note, in force since February 2025, covers government departments, their agencies and the NHS, and calls Cyber Essentials "the quickest and most effective" way to deal with the risk.

Many of these firms work for them

At least 75 of the 420 firms we looked at, nearly one in five, mention public sector clients on the pages of their websites we read: local authorities, the NHS, housing associations, government departments. The real figure is higher, because we only read part of each site.

SOURCES

Supplier reviews. DSIT Cyber Security Breaches Survey 2025/26: micro 12%, small 22%, medium 30%, large 48%.

Policy note. Cabinet Office, PPN 014 Cyber Essentials scheme, for procurements from 24 February 2025. "Since 2014 the government has required suppliers bidding for certain types of public contracts to hold Cyber Essentials or Cyber Essentials Plus certification (or demonstrate that equivalent controls are in place)."

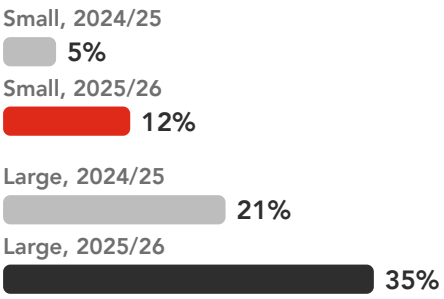
75 firms. AIS Technology analysis of the website text read while vetting the 420 firms, November 2026.

PART ONE · TRUSTED

Few firms can show **the badge**

Cyber Essentials is the government-backed certificate that public buyers name and bigger clients recognise. Small businesses are taking it up quickly, but from a low base: 12% now hold it.

Businesses holding Cyber Essentials



2024/25 against 2025/26, small and large businesses.

A quarter of businesses (24%) say they already have the technical controls in all five areas the scheme checks. Many firms are closer to certification than they think.

The five areas Cyber Essentials checks

01 **Firewalls**
Boundary protection between your devices and the internet.

02 **Secure configuration**
Devices and software set up securely, with defaults changed.

03 **User access control**
The right access for the right people, including multi-factor sign-in.

04 **Malware protection**
Protection against viruses and other malicious software.

05 **Security update management**
Software kept up to date and patched promptly.

> Organisations with Cyber Essentials are 92% less likely to make a claim on their insurance.
>
> NCSC ANNUAL REVIEW 2025, CITING THE CYBER ESSENTIALS INSURANCE PROVIDER

What it costs

10 TO 49 STAFF
£440 + VAT

50 TO 249 STAFF
£500 + VAT

The assessment fee for basic Cyber Essentials, renewed every year. Where a public contract requires it, the certificate has to be renewed annually for the life of the contract.

SOURCES

Uptake. DSIT Cyber Security Breaches Survey 2025/26: small businesses from 5% to 12%, large from 21% to 35%; 24% of businesses report controls in all five areas.

Five areas. NCSC, Cyber Essentials technical requirements.

92%. NCSC Annual Review 2025. The figure comes from insurer claims data and shows a correlation, not proof of cause.

Costs. IASME, Cyber Essentials assessment prices, November 2026. Annual renewal for contracts: PPN 014.



PART TWO

TARGETED: YOUR NAME **ON THE INVOICE**

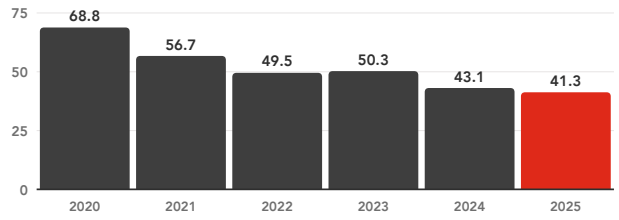
Professional firms send invoices for large sums to clients who expect them. That makes your name worth borrowing. One email with "new bank details" from what looks like your address is all it takes.

PART TWO · TARGETED

Invoice fraud is falling. **It still cost £41m.**

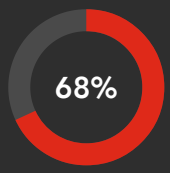
UK Finance counts the losses from invoice and mandate fraud: a criminal intercepts an email, or takes over a mailbox, and tells the payer the bank details have changed. Losses have fallen every year bar one since 2020. They still land hardest on businesses.

Invoice and mandate fraud losses in the UK, £ millions



All victims. 2025 in red.

BUSINESS ACCOUNTS



of invoice and mandate losses in 2025 came out of business accounts: £28m, about £23,000 a case.

01

Get into a mailbox

Yours or your client's. A phished password is enough when there is no multi-factor sign-in.

02

Wait for the invoice

Read the thread quietly until a fee note or stage payment is due.

03

Change one detail

"Our bank details have changed." Sent from your real mailbox, or from an address one letter away.

04

Collect your fee

The client pays the criminal, thinks they've paid you, and the money is gone within hours.

ILLUSTRATION · FICTIONAL FIRM

`accounts@marlowehirstdesign.co.uk` GENUINE

`accounts@marlowehirstdes1gn.co.uk` LOOKALIKE

`accounts@marlowehirst-design.co.uk` LOOKALIKE

SOURCES

UK Finance. Annual Fraud Report 2026: losses £68.8m, £56.7m, £49.5m, £50.3m, £43.1m, £41.3m for 2020 to 2025; "68 per cent (£28 million)" on business accounts; the method "often involves the criminal either intercepting emails or compromising an email account".

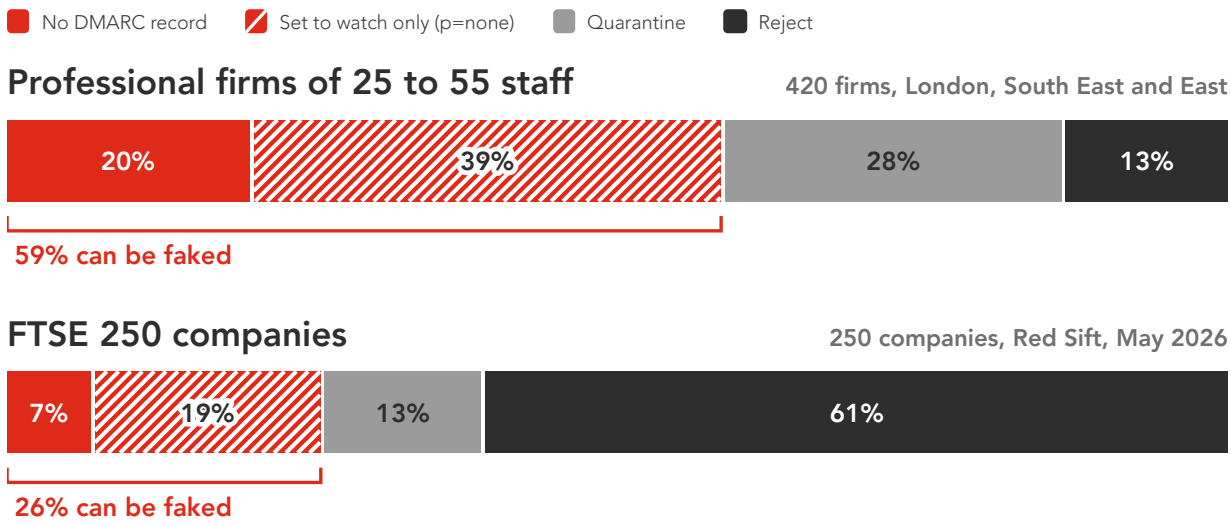
£23,000. Our arithmetic: £28.0m across 1,217 business cases in 2025.

The four steps. Our description of the method UK Finance sets out.

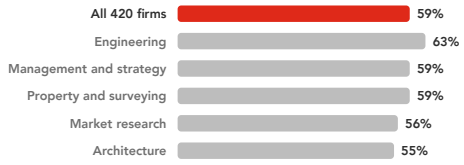
PART TWO · TARGETED

Six in ten firms **can be faked**

One email setting, called DMARC, tells Microsoft, Google and every other provider to reject messages that fake your firm's address. It costs nothing. We read it for 420 professional firms with 25 to 55 staff: 59% either have no record or have it set to "none", which watches and does nothing. For FTSE 250 companies the figure is 26%.



Firms that can be faked, by type of firm



Types with at least 30 firms in the sample.

88 of 162

firms on "watch only" haven't given an address for the reports. Nobody is watching.

34 of 67

firms paying for an email filter such as Mimecast can still be faked. A filter guards your inbox. DMARC guards your name in everyone else's.

SOURCES

Method. Public DNS records read by AIS Technology on 12 Nov 2026, scored on the domain each firm's staff send email from. No firm was contacted and no system was tested. Totals only; no firm is named.

The 420 firms. Professional firms in London, the South East and the East of England with about 25 to 55 staff on LinkedIn and no in-house IT role we could find. 87% run email on Microsoft 365. FTSE 250: Red Sift, 12 May 2026.

PART TWO · TARGETED

What this setting **won't do**

DMARC stops one trick: email that claims to come from your exact address. It does nothing about a lookalike domain, a client's hacked mailbox, or a phone call from someone pretending to be your accounts team. Each trick needs its own defence.

The trick	What it looks like	What stops it
Your exact address, faked	An email that really does show @yourfirm.co.uk as the sender	**DMARC set to reject**
A lookalike domain	One letter changed, a hyphen added, or .com for .co.uk	Clients who know you never change bank details by email, and domain monitoring
A hacked mailbox	A real account, yours or a client's, sending a real-looking fee note	Multi-factor sign-in, and a call to a known number before any payment

CHECK YOUR OWN FIRM IN TWO MINUTES

01 Open any free DMARC lookup site. MXToolbox has one at `mxtoolbox.com/dmarc.aspx`.

02 Type your email domain: everything after the @ in your own address.

03 Read the value after `p=` against the list.

p=reject	Fake email using your address is refused. This is where you want to be.
p=quarantine	Fake email goes to junk. Good, and one step from finished.
p=none	Watching only. Nothing is blocked.
Nothing found	No protection at all.

> Having a DMARC policy of 'reject' on all of your domains is the best way to prevent spoofing of your email.
>
> NATIONAL CYBER SECURITY CENTRE

SOURCES

NCSC. Email security and anti-spoofing guidance, ncsc.gov.uk.

Moving to reject. Set up every service that sends email for you first (your accounts package, your project tools, your newsletter), read the reports for a few weeks, then tighten the policy.



PART THREE

TARGETED: WHEN CLIENT DATA GETS OUT

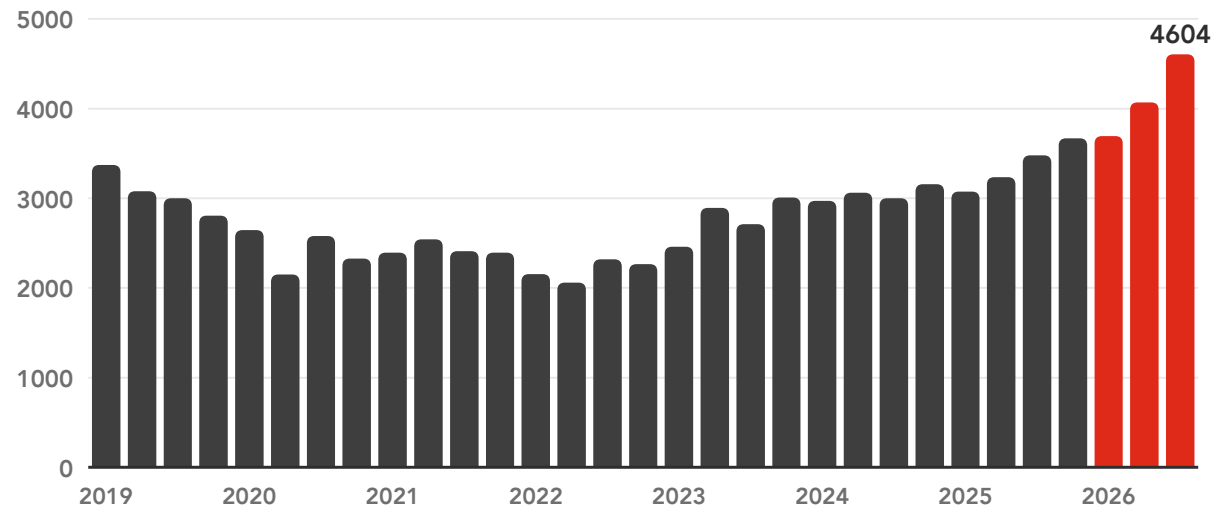
Drawings, reports, survey data, HR files, client accounts. A professional firm holds a great deal of other people's information, and a serious breach has to be reported to the Information Commissioner within 72 hours.

PART THREE · TARGETED

Breach reports are at a **record high**

Across every sector, the ICO received 16,034 data breach reports in the 12 months to September 2026, up 24% on the year before. The third quarter of 2026, with 4,604 reports, was the busiest since the ICO's data begins in 2019. Phishing reports rose by more than half.

Data breach reports to the ICO, all sectors, by quarter



Q1 2019 to Q3 2026. 2026 quarters in red.

+53%
phishing reports to the ICO in a year: 2,134 against 1,398.

36%
of reports reached the ICO more than 72 hours after the organisation found out.

85%
of professional, scientific and technical businesses call cyber security a high priority. Only 41% have a board member responsible for it.

SOURCES

ICO. Data security incident trends, open data Q1 2019 to Q3 2026, published 26 Oct 2026. All sectors, one record per report reference. 12 months to September compares Q4 2024 to Q3 2025 with Q4 2025 to Q3 2026. Analysis by AIS Technology. These are breaches organisations chose to report.

85%, 41%. DSIT Cyber Security Breaches Survey 2025/26, sector results for professional, scientific or technical businesses.

WHAT TO DO

Nine things that move you from targeted **to trusted**

This week

- ✓ **Look up your DMARC setting.**
  Two minutes, using the steps in part two.
- ✓ **Check multi-factor sign-in covers every account,**
  including admin and shared accounts and anything set up years ago.
- ✓ **Tell your clients how you invoice.**
  Your bank details never change by email, and they should call you on a number they already have if they ever see a request that they do.

This month

- ✓ **Find out what your clients ask suppliers.**
  Pull together the security questions from your last few tenders and client onboarding forms, and the answers you gave.
- ✓ **Name who reports a breach,**
  and their deputy. The ICO's 72 hours runs from when you become aware.
- ✓ **Register the obvious lookalikes of your domain,**
  or set up monitoring so you hear when someone else does.

This quarter

- ✓ **Get Cyber Essentials.**
  It covers several of the items on this page and is the certificate public buyers name.
- ✓ **Take DMARC from "none" to "reject",**
  once every service that sends email for you is set up.
- ✓ **Run phishing training with a real test.**
  Phishing reports to the ICO rose by more than half in a year.

Want a second opinion on where your firm stands?

Call AIS Technology and talk it through. We look after the IT of professional firms across Essex, London and the South East.

020 4591 6648

info@ais.london · aistech.co.uk

SOURCES

Cyber Essentials. ncsc.gov.uk/cyberessentials. AIS Technology helps its managed clients reach Cyber Essentials and Cyber Essentials Plus.

A plan template. AIS Technology's free business continuity plan template covers declaring an incident and the 72-hour rule: aistech.co.uk/guides.

SOURCES AND METHOD

Where **every number** comes from

Email settings. Public DNS lookups (DMARC, SPF, MX) through public resolvers on 12 Nov 2026, by AIS Technology, for 420 professional firms. Results published as totals only. A setting shows what a firm has told other providers to do; it doesn't prove that a given fake email would arrive.

Public sector mentions. AIS Technology's reading of the website text collected while vetting the 420 firms, November 2026. Counted only for specific terms such as "public sector", "local authority", "NHS" and named government bodies.

Government survey. DSIT Cyber Security Breaches Survey 2025/26, published 30 April 2026.

Policy note. Cabinet Office, PPN 014 Cyber Essentials scheme (February 2025).

NCSC. Annual Review 2025; Email security and anti-spoofing guidance; Cyber Essentials requirements.

UK Finance. Annual Fraud Report 2026, covering 2025, invoice and mandate scam tables.

ICO. Data security incident trends, open data Q1 2019 to Q3 2026, updated 26 Oct 2026. One record per report reference. Analysis by AIS Technology.

FTSE 250. Red Sift, "FTSE 250 DMARC report", 12 May 2026.

A note on the sample. The 420 firms are professional firms in London, the South East and the East of England with roughly 25 to 55 staff on LinkedIn and no in-house IT role that we could find. They are not a random sample of all UK firms.

This report is general information and isn't legal advice. Figures are correct as at 12 November 2026.

HOW THE NUMBERS WERE BUILT

420

Firms checked

Public email settings for every professional firm in the sample, read on 12 November 2026.

89,591

Reports filtered

The ICO's full breach file, one record per report, for the 16,034 reports in the latest year.

2,112

Businesses surveyed

The base of the government's 2026 Cyber Security Breaches Survey.



ABOUT AIS TECHNOLOGY

IT SUPPORT AND CYBER SECURITY FOR FIRMS THAT **SELL THEIR EXPERTISE**

AIS Technology looks after the IT of professional firms across Essex, London and the South East: Microsoft 365, cyber security, a 24/7 help desk and on-site engineers. Our founder, Chris Dunham, worked in network security for the Home Office and for financial institutions before starting AIS.

We help our managed clients reach Cyber Essentials and Cyber Essentials Plus, so the next client questionnaire is a formality rather than a worry.

If anything in this report raised a question about your own firm, call us. We're happy to talk it through.

CALL

020 4591 6648

EMAIL

info@ais.london

WEB

aistech.co.uk

AIS TECHNOLOGY

Trusted or Targeted? Published by AIS Technology, Wickford, Essex, November 2026. Contains public sector information licensed under the Open Government Licence v3.0. Images are illustrative. This report is general information and isn't legal advice.