



WHITEPAPER

The *Insurance* Reality Check

Why Your Cyber Policy Might Not Pay Out

01 · THE STARTING POINT

A Cyber Policy Is a Promise With Conditions

Buying cover is the easy part. Whether it pays depends on what you told the insurer, what you actually had in place on the day, and what the wording says about the kind of loss you suffered.

37%

of UK businesses say they currently have cyber insurance

Source: Superscript, Cyber-security in 2026 (1,000 UK business owners)

43%

of UK businesses identified a breach or attack in the past 12 months

Source: DSIT, Cyber Security Breaches Survey 2025/26

What a Cyber Policy Usually Contains



Your Own Losses

Business interruption, data restoration and extortion costs



Claims Against You

Liability to customers or others whose data or service is affected



Response Support

Forensics, legal advice and a claims line to call first

What It Rarely Pays For

- ⊗ Regulatory fines. GDPR fines are not insurable in the UK
- ⊗ Attacks the policy excludes, such as war or state-backed activity
- ⊗ Spending you commit to without the insurer's consent

£197m

UK insurers paid this much in cyber claims in 2024, up 230% on the year before. Claims do get paid. The question is whether yours will.

Source: Association of British Insurers, 2024 claims data

02 · HUMAN ERROR

Does Cyber Insurance Cover Human Error?

Often, yes. Insurers expect people to make mistakes. The risk is rarely the mistake itself. It is a mistake made while a required control was missing, or one that lands in a sub-limit.

SCENARIO	TYPICALLY	WHAT TO CHECK IN YOUR POLICY
Accidental deletion or system misconfiguration	Often covered	Does the wording include system failure or human error cover?
A colleague clicks a phishing link and ransomware follows	Usually covered	Were the required controls, such as MFA, in place that day?
A colleague is tricked into paying a fake invoice	Often sub-limited	What is the social engineering limit, and is a call-back check required?
Personal data sent to the wrong recipient	Costs yes, fines no	Are notification and legal costs included in the response cover?
A deliberate act by a dishonest employee	Usually excluded	Ask your broker whether crime cover sits alongside the cyber policy

2x

Voice phishing attacks doubled in a year. A convincing phone call is now one of the likeliest routes to a payment fraud claim.

Source: Marsh, 2026 UK cyber outlook, reported by Insurance Business UK

Cover for funds transfer fraud and business email compromise is typically written as a sub-limit in the UK, not up to your full policy limit. Source: Insurance Business UK.

03 · QUALIFYING

What Is Required to Qualify for Cyber Insurance?

Requirements vary by insurer and by business size, but underwriters keep asking for the same handful of controls. Expect to be asked for evidence, not just a yes or no.



Multi-Factor Authentication

On email, remote access and every admin account



Tested, Offline Backups

A restore that has been proven, with one copy out of reach



Endpoint Protection

Detection and response on every device and server



Patching

Fixes applied promptly to anything facing the internet



Staff Awareness Training

Regular, recorded, and covering payment fraud



An Incident Response Plan

Named roles, contacts and a notification routine

38%

of UK businesses provide regular cyber security training for staff, a gap underwriters notice

Source: Superscript, Cyber-security in 2026 (1,000 UK business owners)



A Route In: Cyber Essentials

Any UK organisation with a turnover under £20m that certifies its whole organisation to Cyber Essentials is entitled to cyber liability insurance arranged by IASME. Certification also shows other insurers that the basic controls are in place.

Source: NCSC, Cyber Essentials

04 · DENIED CLAIMS

Why Are Cyber Insurance Claims Denied?

Most disputes come down to the gap between what was declared and what was true on the day of the incident. Claims teams report paying many claims where an answer was slightly off, but a large loss draws close scrutiny.

1

Answers That Do Not Match Reality

The application said MFA everywhere.
The breached account had none

2

Controls Not Maintained

A condition or warranty required a control that had lapsed

3

Late Notification

The policy sets a deadline to tell the insurer, and it was missed

4

Spend Without Consent

A ransom or major cost was committed before the insurer agreed

5

Missing Evidence

Training, backup or MFA records could not be produced

6

Wrong Cover Section

The loss fell into an exclusion or a low sub-limit

Two Disputes That Made Headlines

Travelers v International Control Services

The insurer said the application described MFA across email, remote access and servers, but it protected only the firewall. It sought to rescind the policy after a ransomware attack.

Columbia Casualty v Cottage Health

The insurer alleged the healthcare provider agreed to maintain minimum risk controls as a condition of cover, and did not, before a data breach.

These are insurers' allegations in US cases, and outcomes differ. Source: published case summaries, Infradapt.

05 · THE REALITY CHECK

Ten Checks Before You Need to Claim

Tick what is true today, then give each gap an owner and a date. Do it before renewal, not after an incident.

- | | |
|--|--|
| ☐ Application answers compared with reality, line by line | ☐ MFA coverage report covers email, remote and admin accounts |
| ☐ Restore test completed and recorded, one copy offline | ☐ Patch records kept for internet-facing systems |
| ☐ Endpoint protection reporting on every device and server | ☐ Social engineering sub-limit known and judged adequate |
| ☐ Insurer notification deadline and claims line saved offline | ☐ Rule agreed: no ransom or major spend without insurer consent |
| ☐ Evidence file ready: training, backup and MFA records | ☐ IT sign-off on every answer at each renewal |

→ Three Steps This Week

- 1** Read your policy schedule and application side by side
- 2** Check MFA covers every account the application mentions
- 3** Ask your broker what your social engineering limit is

Book a Cyber Insurance Readiness Review

We will check your controls against your application before an insurer does

0161 834 9345 | 0115 822 1860
contact@netmonkeys.co.uk