BUSINESS INSIGHTS | CYBER RISK

Cyber Insurance Review Checklist 2026

A practical guide for UK SMEs reviewing ransomware, phishing, data breach response, supplier dependency, business interruption, governance and underwriting evidence before comparing cyber insurance cover.

Primary route: insure24.co.uk/cyber-insurance/ | Guide URL: insure24.co.uk/business-insights/cyber-insurance-review-checklist-2026/

Why this guide was selected

The latest repository-held Google Search Console export, covering 15 August 2026 to 28 August 2026, showed the /cyber-insurance/ page with 2,146 impressions and zero clicks. Related zero-click queries included cyber insurance, cyber insurance brokers, cyber insurance cost, cyber insurance coverage, cyber insurance quotes, cyber insurance comparison, compare cyber insurance and business cyber insurance.

This makes cyber the strongest remaining monthly-download gap in the Business Insights programme. The site already has quote-led cyber pages; this checklist gives directors, managers and brokers a preparation asset that turns search visibility into a practical renewal conversation.

Source-backed context

Source theme	Planning relevance
Cyber Security Breaches Survey 2025/2026	43% of businesses identified a breach or attack; 47% reported being insured against cyber security risks in some way.
Risk and supplier review gap	30% conducted a cyber risk assessment; 15% reviewed immediate supplier risk; 6% reviewed wider supply-chain risk.
Incident response gap	25% of businesses had a formal incident response plan.
Cyber Governance Code of Practice	Directors should identify critical digital processes, agree ownership, set risk appetite and assess supplier risk.

Executive checklist

- Confirm who owns cyber risk at director, partner, trustee or senior-manager level.
- List critical systems: email, website, ecommerce, EPOS, bookings, finance, CRM, payroll, production tools, remote access and cloud storage.
- Describe the data held: customer records, employee data, payment information, health data, confidential client files or member information.
- Check MFA for email, remote access, administrator accounts, finance systems and cloud platforms.
- Record backup frequency, offline or immutable backup controls, restore testing and recovery responsibilities.
- Map suppliers whose outage could stop trading, including IT support, MSPs, payment providers, website platforms and sector software.
- Document prior incidents, near misses, fraudulent payment attempts, phishing campaigns and remediation.
- Prepare day-one incident contacts: directors, IT support, broker, insurer, legal adviser, bank, communications lead and reporting routes.
- Estimate downtime impact for one day without email, one day without payments, one week without core files, and loss of a key supplier platform.

Policy wording questions

Area	Question to ask before comparing quotes
Incident response	Is 24/7 response support available, and who must be contacted first?
Ransomware and extortion	Are response, restoration, negotiation support and related costs covered, subject to law and wording?
Data breach	Are forensic, legal, notification, customer support and third-party liability costs addressed?
Business interruption	What trigger, waiting period, indemnity period, sub-limit and outsourced-service wording applies?
Fraud and phishing	Does the policy address email compromise, social engineering or payment diversion, or is separate crime cover needed?
Security conditions	Are MFA, backups, patching, endpoint controls, remote access and incident notification obligations accurate?
Supplier dependency	Does cloud, payment, website, booking or managed-service failure trigger cover?
Professional services overlap	Could the same event create a professional indemnity allegation?

Scenario prompts for renewal meetings

- Ransomware locks files on Monday morning and the business cannot access billing, schedules or customer records.
- A phishing email compromises a finance inbox and a supplier payment is diverted.
- An ecommerce, booking, EPOS or payment provider outage interrupts revenue during a peak trading period.
- A laptop, mailbox or cloud account containing customer or employee data is accessed without authority.
- An MSP, software vendor or cloud provider suffers an incident that prevents normal service delivery.
- A cyber incident also creates a complaint about professional advice, implementation work or client financial loss.

Broker preparation notes

Use this checklist to collect facts before requesting terms. It should not be used to make controls look stronger than the evidence supports. If a control is absent, unclear or only partly implemented, record that position accurately and discuss remediation before submission where it is material.

The most useful comparison is not simply the lowest premium. Compare the quoted wording against the business model, critical systems, supplier dependencies, realistic downtime scenarios, data exposure, response support, exclusions and security conditions.

Board-level review questions

- Which digital services are essential for revenue, customer service, safety, compliance or payroll?
- Who is accountable for cyber risk and who can make decisions during an incident?
- What level of outage, data loss or financial exposure is tolerable before insurance and controls are reassessed?
- Which third parties are critical, and what evidence is held about their resilience?
- Has the incident plan been rehearsed, and does everyone know the first three calls to make?
- Does the selected limit support response, recovery, interruption, legal, liability and communication costs?

Internal links for further review

- Cyber insurance: insure24.co.uk/cyber-insurance/

- Cyber insurance quotes: insure24.co.uk/cyber-insurance-quote/
- Cyber insurance cost: insure24.co.uk/cyber-insurance-cost/
- Cyber liability insurance: insure24.co.uk/cyber-liability-insurance/
- Small business cyber insurance: insure24.co.uk/small-business-cyber-insurance/
- Cyber risk assessment: insure24.co.uk/cyber-insurance/risk-assessment/
- Cyber business interruption: insure24.co.uk/cyber-insurance/business-interruption/
- Cyber insurance providers UK: insure24.co.uk/cyber-insurance/providers-uk/

Sources

- GOV.UK Cyber Security Breaches Survey 2025/2026, published 30 April 2026.
- GOV.UK Cyber Governance Code of Practice, published 8 April 2025.
- NCSC Small organisations guide to cyber security, published 9 April 2026 and reviewed 21 July 2026.
- NCSC Small Business Guide: Response and Recovery.
- GOV.UK Cyber Resilience Pledge, updated 13 July 2026.