CYBER INSURANCE Readiness Guide for UK SMES 2026

What underwriters actually require, what gets you declined, and how to prepare for renewal

A practical guide for business owners, finance directors and IT leaders

THE RENEWAL YOU DIDN'T SEE COMING

Cyber insurance renewals are getting tougher. Carriers want evidence of MFA, EDR, immutable backups, and patching discipline before they'll quote. The gap between 'we have insurance' and 'we have evidence' is where premiums double or applications get declined.

The shift is structural. Insurers paid out heavily through the ransomware boom of 2020–2023 and have spent the years since tightening underwriting. Carriers that once accepted a tick-box questionnaire now ask for documentary evidence. MFA, EDR, tested backups, and incident response plans have moved from "nice to have" to "required for cover".

Businesses without them either pay materially more typically a 50–100% premium increase or are declined and find themselves shopping for a new carrier on short notice.

Enforcing controls like MFA and backups is no longer enough; carriers want to see when and how they are tested, so businesses arriving unprepared risk declined coverage or higher premiums.

This guide explains what underwriters now actually require, how to improve your renewal success, and how to secure better coverage and premiums.

Use this guide as

- A pre-renewal preparation checklist start 90 days before expiry.
- A briefing document for your IT team or MSP on what the insurer needs.
- A diagnostic on whether your current controls are insurable in 2026.
- A reference for what a strong renewal pack looks like.

Cyber insurance renewal coming up?
We offer a free Cyber Insurance Readiness Review, we'll assess your current posture against the controls insurers actually require, identify gaps that could affect your premium or coverage, and give you a prioritised plan to close them in time. Most useful 90 days before renewal; still valuable at 60 or 30 days. Free of charge, completed within five working days.

- Request your free Insurance Readiness Review at systemforce.co.uk

WHY THE CYBER INSURANCE MARKET HAS HARDENED

Cyber insurance is a young market by insurance standards modern policies barely existed twenty years ago. Through the late 2010s and early 2020s, carriers wrote business aggressively, with broad coverage and modest premiums.

The ransomware boom of 2020–2023 broke the model. Loss ratios spiked. Some carriers exited the market entirely. The ones who stayed rebuilt their underwriting from the ground up.

Three changes from that period are now baked into how UK SMEs are underwritten in 2026:

1. **Controls evidence, not controls assertion**
   Carriers now expect documentary evidence Conditional Access policy exports, EDR reports, and restore test records-so you can feel assured your efforts are recognized and trusted.

2. **Pre-binding scans and post-binding monitoring**
   Some carriers now run external attack-surface scans on prospective insureds before binding cover and continue monitoring afterwards. A new exposed RDP port, an unpatched VPN appliance, and an SMB share visible from the public internet these now trigger underwriter calls during the policy term, not just at renewal.

3. **Sub-limits and exclusions where there used to be limits**
   The cover available has narrowed. Specific exclusions for war and state actors are now standard. Sub-limits on ransomware payments are common. Coverage for social engineering and BEC has tightened. The headline policy limit is still there; what's covered under that limit is much more carefully defined.

> The hardest part of cyber insurance renewal in 2026 is ensuring your quote covers your needs at an affordable premium, empowering you to feel prepared and confident before your policy lapses.
>
> - Recurring observation from broker conversations

WHAT UNDERWRITERS NOW REQUIRE

The list below summarises the controls underwriters in the UK SME market routinely require. Specific carriers vary, and high-coverage policies demand more than entry-level ones. Where the table says "mandatory", it means most carriers will decline coverage or impose material premium increases without it. Where it says "increasingly required", it means the trend is clear, and the requirement will be standard within 12 months.

Requirement	What underwriters actually want	Typical status
MFA universal	Enforced via Conditional Access on every account, every application including admin and remote access. Per-user MFA toggles do not count.	**Mandatory**
EDR / next-gen AV	Endpoint Detection and Response on every endpoint, with monitoring. Not legacy signature-based antivirus.	**Mandatory**
Backup tested & immutable	Backup of all critical data, with at least one immutable copy. Tested restore evidence within the last 90 days.	**Mandatory**
Patch management	Critical patches applied within 14 days, documented process. End-of-life software removed or risk-accepted.	**Mandatory**
Incident response plan	Documented, with named owners, contact lists, and decision authority. Rehearsed at least annually.	**Mandatory**
Awareness training	Continuous programme not just induction. Phishing simulation evidence is increasingly required.	**Increasingly required**
Network segmentation	Particularly for businesses with sensitive data, OT/IT separation, or regulated workloads.	**Sector-dependent**
Privileged access controls	Separate admin accounts, MFA on admin (FIDO2 increasingly preferred), and monitor admin activity.	**Increasingly required**
Email security	DMARC at p=reject, advanced threat protection (Defender for O365 or equivalent) configured.	**Increasingly required**
Vendor/supply chain	Documented review of critical IT suppliers, particularly MSPs, awareness of supply-chain risk.	**Emerging requirement**

What this means in practice: an SME without MFA universally enforced, EDR deployed, tested backups, and a documented incident response plan will struggle to obtain meaningful cyber insurance in 2026. The cover may technically exist, but premiums will be punitive, exclusions extensive, and renewal a year later increasingly uncertain. Remediation is well within reach for most businesses; the cost of remediation is almost always lower than the cost of declined or restricted cover.

Cross-reference: the System Force Cyber Security Framework white paper covers each of these controls in detail. The Cyber Essentials, Backup & DR, and Microsoft 365 guides are the operational playbooks for individual control areas.

WHAT DRIVES YOUR PREMIUM UP / AND DOWN

Premium changes at renewal are not arbitrary. Underwriters apply largely consistent factors when calculating the renewal premium, and most of those factors are within the customer's control. The table below summarises the factors we see most consistently and what you can do about them.

Factor	Effect on premium	What you can do about it
MFA gaps	+30–80% or decline	Close every gap before renewal especially admin and service accounts.
Legacy AV (no EDR)	+20–50% or decline	Deploy EDR at least 60 days before renewal long enough to be defensible.
No tested backup	+20–60%	Run a documented restore test; keep evidence in the renewal pack.
Sector/size	Variable	Cannot change. Mitigate with strong controls and evidence.
Prior incident	+50–200% or decline	Show post-incident remediation. Documentation matters.
Cyber Essentials	−5–15%	Achieve and maintain. Discounts vary by carrier but are consistently positive.
ISO 27001	−10–25%	Premium-grade discount. Worth pursuing for serious operations.
Strong renewal pack	−5–15%	Documentation alone without changing controls is worth real money.

The optimisation pattern: businesses that prepare seriously for renewaclosing the gaps that drive increases, securing the qualifications that drive discounts, presenting the documented evidence that builds confidence typically achieve renewal premiums 20–40% lower than businesses that submit the same controls without the preparation work. Preparation is one of the highest-ROI activities in modern cyber insurance.

WHAT GETS YOU DECLINED / AND WHAT TO DO ABOUT IT

Outright decline is no longer rare in the UK SME cyber insurance market. The patterns below are the ones most consistently associated with declined renewals. None of them is catastrophic individually; most can be resolved within 90 days with focused effort.

- MFA is not enforced for all users (admin gaps are the most common reason).
- Legacy antivirus instead of EDR, no detection and response capability.
- Backups untested no evidence that a restore would work.
- End-of-life operating systems still in production (Windows 7, Server 2012, etc.).
- RDP or other admin services are exposed directly to the internet.
- Recent material incident with no documented remediation evidence.
- No documented incident response plan or one that hasn't been updated in years.
- An unpatched, unsupported VPN appliance or firewall is the perimeter.
- "We don't know" answers to the proposal form declined is sometimes preferred to misrepresented.

The pattern: most declines we see trace to two or three of the items above, often known to the business but never escalated until the renewal hit. Underwriters are not unreasonable; they will work with businesses willing to commit to remediation timelines. "We will have EDR deployed by 1 July" is a more useful answer than "we don't have EDR". A documented remediation plan, even if not yet executed, sometimes secures cover where its absence would not.

YOUR 90-DAY RENEWAL PREPARATION TIMELINE

Cyber insurance renewal is a project, not a form. The businesses that achieve good renewal outcomes start the work 90 days before the policy expires not the week before. The plan below provides a realistic structure.

Days 90–60 / Diagnose

- Pull the current policy and proposal form. Re-read it as if you were the underwriter.
- Identify every control statement that is now technically incorrect or undocumented.
- Run a self-assessment against the requirements table in this guide.
- Engage your IT provider or internal team share what's needed and the timeline.
- Brief leadership on likely renewal trajectory if no remediation is undertaken.

Days 60–30 / Remediate

- Close MFA gaps particularly admin accounts, service accounts, and legacy applications.
- Deploy or upgrade EDR if relying on legacy antivirus.
- Run a restore test against existing backups document the outcome.
- Update or write the incident response plan; brief named owners.
- Resolve any internet-exposed admin services (RDP, admin portals, legacy VPN).
- Begin awareness training programme if absent even basic deployment counts.

Days 30–0 / Document and present

- Compile the renewal pack see the next page for the recommended contents.
- Run a tabletop exercise on the IR plan; document the date and outcome.
- Take screenshots and policy exports as evidence.
- Brief your broker fully give them ammunition for the underwriter conversation.
- If a meaningful gap remains, prepare the remediation commitment letter.

Realistic outcome: an SME starting at "some MFA, basic AV, untested backup, no IR plan" and executing this 90-day plan typically arrives at renewal with a defensible posture, a complete documentation pack, and a premium 30–50% lower than the alternative trajectory of doing nothing. The remediation cost is usually less than 12 months of the premium difference. The arithmetic is straightforward.

Renewal in less than 90 days?
There's still time. Many of the highest-impact remediation actions MFA enforcement gap closure, EDR deployment, restore testing, and IR plan documentation, can be completed within 30 days with focused effort. Even at 14 days out, a documented remediation commitment can shift the underwriter conversation. We routinely help SMEs through tight renewal timelines.

- Book an urgent renewal preparation call at systemforce.co.uk

WHAT A STRONG RENEWAL PACK CONTAINS

A well-prepared renewal pack is documentation that proves the controls described on the proposal form actually exist, are configured correctly, and are operationally maintained. It transforms the underwriter conversation from "we'll have to take their word for it" into "the evidence speaks for itself".

#	Document	Why it matters
1	MFA enforcement evidence (Conditional Access policy export)	Proves universal enforcement, not just "enabled".
2	EDR deployment report (coverage % across endpoints)	Demonstrates active protection, not legacy AV.
3	Latest restore test record (date, scope, outcome)	Differentiates "backup" from "recoverable".
4	Patch compliance report (last 90 days)	Shows operational discipline, not just policy.
5	Incident response plan (current version)	Demonstrates preparation; many SMEs don't.
6	Most recent IR tabletop exercise summary	Evidence that the plan is practised, not theoretical.
7	Awareness training programme description + completion stats	Increasingly demanded programmes beat one-off training.
8	Phishing simulation results (last 6 months)	Quantifies the human-layer defence.
9	Cyber Essentials / ISO 27001 certificate (if held)	Material premium discount with most carriers.
10	Vendor / MSP risk review summary	Increasingly required for supply-chain due diligence.

The non-obvious value: compiling the renewal pack itself surfaces gaps. Businesses sit down expecting to assemble what they have and discover halfway through that the EDR coverage report shows 87% deployment, or the last restore test was 18 months ago, or the IR plan still names a director who left in 2023. Better to find that out four weeks before renewal than four weeks after a claim. The exercise of producing the pack is part of the value, not just the output.

COMMON RENEWAL FAILURES (AND HOW TO AVOID THEM)

These are the recurring patterns we see in SMEs whose cyber insurance renewals go badly. Each is avoidable; together they account for most of the bad outcomes we encounter.

- Starting the renewal process two weeks before expiry too late for any meaningful remediation.
- Misrepresenting controls on the proposal form even unintentionally, even by a single word.
- Treating the proposal form as the broker's job, not the IT team's answers should be evidence-based.
- Not engaging IT in the renewal conversation the people who know the controls aren't asked.
- Ignoring the renewal questionnaire's open questions "please describe" answers are where premiums are won and lost.
- No renewal pack the underwriter has nothing to work with beyond raw answers.
- Single-carrier renewal no comparison quotes, no negotiating leverage.
- Not pursuing Cyber Essentials the discount is real, and the work is modest.
- Believing "we've never had an incident" replaces evidence carriers underwrite forward, not backwards.

The pattern: almost every cyber insurance renewal that goes badly traces to under-preparation. Renewal is a 90-day project, not a one-week task. Businesses that treat it that way achieve materially better outcomes than businesses that don't.

HOW SYSTEM FORCE IT CAN HELP

IT and security partner that delivers the controls, evidence, and documentation underwriters now require. Our clients consistently achieve better renewal outcomes than businesses doing the same work in-house, because the work is recognisable to us and we know what underwriters are looking for.

System Force IT delivers:

- Cyber Insurance Readiness Reviews assessment against current underwriter requirements, with prioritised remediation plan.
- Pre-renewal remediation closing gaps in MFA, EDR, backup, patching, awareness, and IR planning.
- Renewal pack preparation compiling the documentation underwriters now expect.
- Cyber Essentials and Cyber Essentials Plus direct premium impact at most carriers.
- ISO 27001 alignment for businesses ready for the next step.
- Ongoing managed security maintaining the controls between renewals so the next one is easier than the last.

Book a free Cyber Insurance Readiness Review.
One of our security consultants will assess your current cybersecurity posture against the controls underwriters now require, identify the gaps most likely to affect your premium or coverage, and provide a costed remediation plan with realistic timelines. Most useful 90 days before renewal; still valuable closer in. Free of charge, fully confidential, completed within five working days.

- Book your free Insurance Readiness Review at systemforce.co.uk

Or call us directly: 01452 701355 We're based in Gloucestershire and prepare UK SMEs for the renewal that matters most.

Authoritative sources and further reading

- UK Cyber Security Breaches Survey: gov.uk/government/statistics/cyber-security-breaches-survey
- NCSC Guidance: ncsc.gov.uk
- Cyber Essentials (IASME): iasme.co.uk/cyber-essentials
- Lloyd's Cyber Market reports: lloyds.com
- ABI cyber insurance guidance: abi.org.uk

Companion resources

- The System Force Cyber Security Framework (white paper).
- Cyber Essentials Readiness Checklist.
- Microsoft 365 Security Quick Wins.
- Backup & Disaster Recovery Checklist.
- UK SME Phishing Defence Playbook.

This document is provided for general guidance only. Premium ranges, decline rates and underwriter requirements cited are typical UK SME observations as of mid-2026; outcomes vary materially by carrier, sector, business size, claims history and policy terms. Always work with a qualified insurance broker for binding advice on cover. This is not insurance advice.

System Force I.T.
Secure IT Simplified

Want a free Cyber insurance readiness review with System Force IT?

We run free, no-obligation reviews for UK SMEs.
Written report in 7 working days.
No sales pitch, no follow-up unless you ask for one.

Book at systemforce.co.uk
Or call us directly: 01452 701355

System Force IT | supporting UK businesses since 2006.

UKAS ISO/IEC 27001: 2022 Certified | Microsoft Solutions Partner | Certified 3CX Partner | Cyber Essentials Practitioners | RIPE NCC Member

Next Step:

Book your free CYBER INSURANCE Readiness Guide for UK SMEs.

01452701355

www.systemforce.co.uk

sales@systemforce.co.uk