DefineEdge

What Cyber Insurance Actually Asks For

Translating insurance-application jargon into plain English

Cyber insurance applications ask a lot of technical questions in insurance language. Underneath the jargon, every question maps to a real-world scenario the insurer has seen play out before. Here's what they're really asking.

MFA Everywhere

Not just email - remote access and any account with administrative rights. A stolen password with no second factor is one of the most common ways breaches start.

Endpoint Detection and Antivirus

Whether anything actually notices and stops malware, on every device that touches business data - not just a basic antivirus that hasn't been checked in years.

Backups - Tested and Immutable

Whether recovery has actually been proven to work, and whether at least one copy can't be reached or deleted by an attacker. A backup that's never been tested is a hope, not a plan.

Patch Management

Whether known security holes are getting closed on a schedule, especially the critical ones. Unpatched systems are one of the easiest ways in.

Employee Security Training

Ongoing awareness and phishing simulation - not a one-time onboarding video. People are still the most common entry point for attackers.

Incident Response Plan

A written plan naming who does what, reachable even if systems are down. Carriers want to know a breach won't turn into chaos on top of a crisis.

Why This Matters

None of these controls are exotic. They're the baseline carriers now expect before offering favorable terms - and going through an application line by line is a useful exercise even if you're not shopping for a new policy, because it's a fast way to see where the real gaps are.

How to Use This

Read this before your next application or renewal so the questions aren't a surprise, and use it as a checklist to talk through with whoever manages your IT. It's not a substitute for the actual application or for advice from your insurance broker.