

GUIDE

Your cyber insurance application is a promise

What you tell your insurer is in place should match your policies and what the board is told. When it does not, coverage can be at risk.

Current as of October 13, 2026 · 3 minute read

Every cyber insurance renewal asks the institution to describe its controls: multi-factor authentication, backups, endpoint detection, patching, privileged access. Those answers are representations. If they turn out to be untrue, an insurer may argue the policy should never have been issued.

Boards rarely see the application. They see the policy summary and the premium. Yet the application is often the most specific statement the institution makes about its controls, made to a party that will check it after a loss.

What has happened

In 2022, after a ransomware attack at International Control Services, Travelers asked a federal court to rescind the cyber policy it had issued. The application said multi-factor authentication protected email, remote access, endpoints, servers and other systems. Travelers alleged it protected only the firewall. The court granted rescission in August 2022 (Travelers Property Casualty Co. of America v. International Control Services, C.D. Ill., No. 2:22-cv-02145).

Earlier, in a case over a 2013 hospital data breach, the insurer argued that the application had misstated how the hospital handled default settings, security patches and vendors (Columbia Casualty v. Cottage Health System). We found no final ruling, but the argument is the point: the application is read closely when there is a claim.

What insurers now ask about

Brokers report that insurers treat a set of controls as a minimum. Marsh lists twelve:

- multi-factor authentication for remote and privileged access;
- email filtering and web security;
- secured, encrypted and tested backups;
- privileged access management;
- endpoint detection and response;
- patch and vulnerability management;
- incident response planning;
- security awareness training and phishing tests;
- hardening remote desktop access;
- logging and monitoring;
- replacing or protecting end-of-life systems;
- supply chain risk management.

Three things to check every renewal

- 1 Does each answer on the application match what your own policies say? If the application says backups are tested quarterly and the policy says annually, one of them is wrong.
- 2 Does it match what the board has been told? The board should not learn about a control gap from a claim denial.
- 3 Who completed and signed it, and who reviewed it before it went to the insurer?

BoardAlign asks for your insurance application and checks it, line by line, against your policies and your board reporting. Where the three disagree, the readout says so. We state what the documents say; we never say whether a claim would be paid.

Sources

Travelers v. International Control Services, docket (C.D. Ill. 2:22-cv-02145).

<https://dockets.justia.com/docket/illinois/ilcdce/2:2022cv02145/86760>

Covington, Inside Privacy, on Columbia Casualty v. Cottage Health (2016). <https://www.insideprivacy.com/data-security/cybersecurity/cyber-insurer-seeks-to-void-data-breach-coverage-because-of-purported-misstatements-in-policy-application/>

Marsh, Cyber resilience: twelve key controls.

<https://www.marsh.com/ca/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html>

General information for directors, not legal advice. Current as of October 13, 2026. Rules change: check the cited source before relying on it.