

EXECUTIVE PAPER · INFRASTRUCTURE

Cyber Insurance Renewal Is a Controls Audit

Underwriters price cyber cover on a handful of named security controls, and insurers have refused to pay when the application overstated them. CFOs and CTOs should run the renewal together, with evidence behind every answer.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CFO, CTO, CEO · 12 min read

AT A GLANCE

The problem. Cyber premiums have fallen for more than three years and new capacity is easy to find, so renewals feel routine. The application behind the policy is not routine. It asks yes or no questions about multifactor authentication, endpoint detection, backups, patching and privileged access, and an insurer can rescind the policy or deny a claim when an answer turns out to be wrong. One manufacturer lost its entire policy over MFA on a single server. A Canadian city paid an $18.3 million recovery bill itself because MFA was only partly deployed.

Why it persists. Finance or the broker owns the renewal. The person who signs the application rarely sees the systems, and the engineers who run the systems rarely see the application. Answers describe policy and intent, while insurers judge what was enforced on the day of the attack.

The recommendation. Make the CFO and CTO joint owners of the renewal. Treat each application question as a control with an owner, written evidence and a test. Fix the gaps before signing, or disclose them. Re-check the same controls every quarter so the answers stay true for the whole policy year.

The Decision in Front of You

Most companies renew cyber insurance the way they renew property cover. The broker sends a questionnaire, someone in finance or IT fills it in, an officer signs it, and the policy binds. The decision is whether that signature is an administrative step or a statement of fact about your security that the business is prepared to defend in court.

The stakes are the whole limit. A policy that pays $10 million after a ransomware attack is worth nothing if the insurer can show that a control you said existed did not.

Market conditions make this easy to overlook. Marsh's Global Insurance Market Index for the third quarter of 2026 shows cyber rates down 4% worldwide, the thirteenth consecutive quarterly decline, with US rates flat and new capacity letting many buyers broaden cover and lower their retentions [3]. Cheap cover makes renewal look like a pricing exercise.

What's Happening

The market is larger, cheaper and more selective about controls

The US market has roughly tripled in five years. The NAIC's 2026 report puts 2025 US direct written premium at about $9.46 billion including alien surplus lines insurers, up 3.5% on 2024 [4]. Domestic insurers wrote nearly $7.5 billion, against $2.75 billion in 2020, and domestic policies in force rose 33%

to about 5.8 million [5]. The industry loss ratio worsened to 53 in 2025 from 48.7 in 2024, and claim severity rose for large and medium businesses [5]. Munich Re estimates the global market at nearly $15 billion in 2025 and expects around $28 billion by 2030 [7].

Claims data shows where losses come from. Coalition's 2026 Cyber Claims Report, drawn from more than 100,000 policyholders in five countries, found claim frequency up 3% in 2025 while average severity fell 19% to $116,000 [6]. Initial ransom demands rose 47%, and a record 86% of ransomware victims did not pay [6]. Businesses with more than $100 million in revenue filed claims five times as often as smaller ones [6].

Underwriters ask about specific controls

Brokers and insurers have converged on a short list. Marsh's twelve key controls start with MFA for remote and privileged access, email filtering, secured and tested backups, privileged access management, endpoint detection and response (EDR, software that records and blocks malicious activity on each machine), and patch management [8]. Marsh says the adoption of certain controls "has now become a minimum requirement of insurers" [8]. The same controls appear in CISA's #StopRansomware Guide, which tells organizations to keep offline, encrypted backups, test them, and implement phishing-resistant MFA for all services [14].

The list rests on claims data. Marsh McLennan paired its claims records with its clients' security self-assessments in 2023 and measured which controls predicted fewer incidents [9]. Organizations that applied hardened baseline configurations to servers were nearly six times less likely to have an incident. MFA reduced the likelihood only when it covered all critical data, all remote logins and all administrator accounts. Patching high-severity flaws within seven days halved the probability of an event, and only 24% of the organizations studied did it [9].

Three cases show what a wrong or missing answer costs

International Control Services, 2022. Travelers issued a cyber policy to an Illinois electronics manufacturer whose application stated that it used MFA to protect administrative access [1][2]. After a ransomware attack in May 2022, Travelers' investigation found MFA protected only the firewall and not the server that was attacked [1]. Travelers sued on July 6, 2022, saying it would not have issued the policy had it known [1]. The company agreed to a judgment rescinding the policy from inception, entered on August 26, 2022 [1]. No claim under that policy, past or future, was covered. The lesson is that materiality attaches to the application as a whole. An answer that was true for the firewall and false for one server was enough.

City of Hamilton, 2024. Ransomware hit the Ontario city on February 25, 2024. The city refused to pay the ransom and spent $18.3 million on response and recovery, about $14 million of it on outside experts [10]. Its insurer denied the claim because MFA "had not been fully implemented at the time of the attack," and the policy excluded losses where the absence of MFA was the root cause [10][11]. City staff

told council that the insurer had recommended MFA in late 2022 [10]. The rollout was under way and incomplete. Taxpayers carried the full bill [11]. The lesson for the CFO: an exclusion tied to a named control turns a deployment schedule into a coverage question.

Jaguar Land Rover and Marks & Spencer, 2025. Two large UK attacks in 2025 show the difference cover makes. Jaguar Land Rover's factories stopped from September 1, 2025 for five weeks. The company was still negotiating a cyber policy through its broker when the attack hit, and the deal was not complete [12]. JLR booked about £260 million of costs by February 2026 with nothing recovered from insurers, the UK government provided a £1.5 billion loan guarantee, and the Cyber Monitoring Centre estimated the cost to the UK economy at up to £1.9 billion [12]. Marks & Spencer, attacked in April 2025, put its total cost at about £136 million and claimed up to £100 million on its cyber policy [13]. The policy absorbed most of the direct cost. Its half-year profit still fell 55.4% [13].

SIDEBAR: WHAT "RESCISSION" MEANS

A denied claim leaves the policy in force for other events. Rescission unwinds it as if it had never existed, usually with the premium returned. Insurers seek it when an application misstated a fact that would have changed their decision to write the risk. In the ICS case the stipulated judgment voided cover for past, present and future claims [1]. The officer who signed the application signed for the whole company's security posture.

Why the Usual Approach Fails

Renewal is run as a procurement task. The broker manages the market, finance manages the budget, and the application is completed under deadline by whoever can answer fastest. That process produces answers that describe policy. "Do you require MFA for all remote access?" gets a yes because the policy document says so. The insurer reads the same yes as a statement that no remote access path exists without MFA.

The questions are written in absolutes and the estates they describe are not. Every mid-size company has a forgotten VPN appliance, a vendor support account, a legacy server that cannot run the EDR agent, or a backup repository reachable with the same domain credentials as everything else. The person signing does not know these exist. The engineers who know have never read the application.

Evidence is assembled after the loss. Forensic investigators working for the insurer reconstruct what was enforced on the day of the attack, from logs and configuration. In both the ICS and Hamilton cases the gap surfaced during the claim [1][10]. Few companies run that reconstruction on themselves before they sign.

Controls drift during the year. An application signed in March describes March. Acquisitions, new SaaS tools, contractors and emergency exceptions add unprotected access over the following months. Some policies, like Hamilton's, tie cover to a named control at the time of the loss [10], and few companies

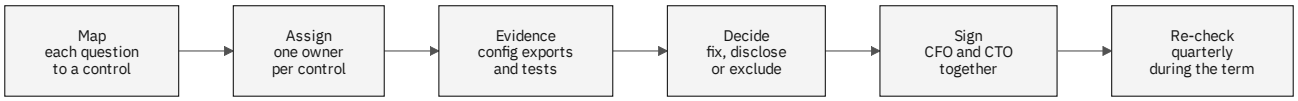
check in September whether the March answers still hold.

Insurers now measure some of this from outside. Coalition routinely scans policyholders for exposed remote access appliances after its claims data linked certain VPN and firewall devices to higher claim frequency [16]. The insurer can see the internet-facing half of your estate whether or not the application describes it accurately.

The Framework: Attest, Evidence, Maintain

Run the renewal as a controls audit with two signatures. The CFO owns the commercial terms and the accuracy of the application. The CTO owns the controls and the evidence. Neither signs alone.

Exhibit 1. The renewal as a controls audit: every answer has an owner and evidence before anyone signs



Source: author's framework, built on Marsh's key controls [8] and CISA's #StopRansomware Guide [14].

Map. Start from last year's application and the draft for this year. Turn every question into a control statement with a defined scope. "MFA on all remote access" becomes a list of every remote access path: VPN, remote desktop gateways, vendor portals, cloud consoles, email.

Assign. One engineer owns each control and its evidence. The owner reads the exact wording of the question.

Evidence. For each control, produce something an investigator would accept: a configuration export showing MFA enforced on every path, an EDR console report showing coverage against the asset inventory, a log of the last restore test from immutable backups, patch reports for internet-facing systems. Test the control as well. Try to log in to each remote path without a second factor. Restore a system from backup.

Decide. Where a control is incomplete, there are three honest choices. Fix it before binding. Disclose it to the underwriter with a dated remediation plan. Or accept an exclusion. The fourth choice, answering yes and hoping, is the one that voided ICS's policy [1].

Sign. The CFO and CTO both sign an internal attestation that the application matches the evidence file. The officer who signs for the insurer then has a record of how each answer was established.

Maintain. Re-run the evidence for the top controls every quarter. Report exceptions to the audit or risk committee the same way finance reports control deficiencies.

Exhibit 2. Five controls underwriters weigh most, and the evidence that proves each

Control	What the application usually asks	Evidence to keep on file	Common gap found after a loss
MFA	Required for all remote access, email and privileged accounts	Export of conditional access or VPN policy; list of every remote path with MFA status; failed bypass test	Vendor support portals, legacy VPNs, service accounts, one admin server [1][10]
EDR	Deployed on all endpoints and servers, monitored 24/7	Agent count reconciled to asset inventory; monitoring contract or on-call rota	Servers too old for the agent; monitoring that alerts nobody after hours
Backups	Offline or immutable, encrypted, tested	Immutability settings; last restore test with time taken; separate credentials	Backups on the same domain as production, encrypted with it [14]
Patching	Critical flaws fixed within a set number of days	Patch age report for internet-facing systems; CISA known-exploited list status	Edge appliances and unsupported systems outside the patch cycle [9]
Privileged access	Admin rights restricted, separate admin accounts	Count of domain admins; access review sign-off	Shared admin passwords; standing access for former staff and contractors

Source: author's analysis of Marsh's key controls [8], Marsh McLennan's 2023 control study [9], CISA guidance [14] and the cases above.

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of running renewal as a controls audit

Area	Cost or risk	Mitigation
Engineering time	Author's estimate: two to four weeks of senior engineering effort in the first year to build the evidence file	Reuse it for SOC 2, ISO 27001 or customer questionnaires; later years cost a fraction
Disclosure	Honest answers may raise the premium, raise the retention or add an exclusion	A known exclusion is cheaper than a rescinded policy; disclose with a dated fix plan
Remediation spend	Closing gaps such as MFA on legacy systems costs money before renewal	Prioritize controls insurers name and claims data supports [8][9]; isolate what cannot be fixed
Officer exposure	Two signatures make two executives accountable	Accountability is the point; back each signature with the evidence file
Timeline	Starting late compresses the audit and pressures teams to answer yes	Start 120 days before the renewal date
When this is wrong	A small business with no in-house systems and a simple package policy gets little from a formal audit	Answer the short form carefully with the outsourced provider, confirm MFA and backups in writing, and keep the confirmation

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Pull the current policy, application and any exclusions tied to named controls. Map every application question to a control and an owner. List every remote access path and every admin account.	CFO with CTO	Question-to-control map complete; remote access inventory signed off
First 90 days	Build the evidence file for MFA, EDR, backups, patching and privileged access. Run bypass tests on each remote path and a full restore from immutable backup. Fix gaps or prepare written disclosures.	CTO with security lead	Evidence on file for all five controls; zero remote paths without MFA, or each one disclosed
First 90 days	Brief the broker on findings before submission. Compare exclusions and warranties across quotes, not only price and limit.	CFO with broker	Application submitted with both signatures and the evidence index attached internally
First 365 days	Re-run evidence quarterly. Add new systems, acquisitions and vendors to the map as they arrive. Report control exceptions to the audit committee. Map the evidence to NIST CSF 2.0 [15] so one file serves auditors and insurers.	CTO with risk or internal audit	Four quarterly attestations; next renewal application completed from the file in under two weeks

Source: author's recommendation.

Questions to Ask Your Team

1. Who signed our last cyber insurance application, and what did they check before signing?
2. Which answers on the application are absolute ("all", "every", "always"), and can we prove each one today?
3. How many ways can someone reach our network or email from outside, and which of them do not require a second factor?
4. Does our policy exclude or limit losses where a named control such as MFA was missing?
5. When did we last restore a production system from backup, and could ransomware reach that backup with stolen admin credentials?
6. Which servers or appliances cannot run our EDR agent or receive patches, and did we disclose them?
7. What changed in our environment since the last application: acquisitions, new vendors, new remote access?

8. If the insurer's forensic team arrived tomorrow, what would they find that contradicts our application?

Closing

A cyber policy is a promise from the insurer that depends on promises from you. The insurer's side is written by lawyers and priced with claims data. Yours is often written in an afternoon by someone who has never seen the firewall configuration. Make the CFO and CTO joint owners of the renewal, prove every answer with evidence before signing, fix or disclose what is missing, and keep the answers true through the policy year.

Sources

[1] Lockton. "Travelers v. ICS underscores need to respond carefully to cyber insurance application questions." 2022. https://global.lockton.com/us/en/news-insights/travelers-v-ics-underscores-need-to-respond-carefully-to-cyber-insurance.

[2] Insurance Journal. "Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use." Travelers Property Casualty Co. of America v. International Control Services Inc., No. 22-cv-2145 (C.D. Ill.). 2022. https://www.insurancejournal.com/news/national/2022/07/12/675516.htm.

[3] Marsh. "Global commercial insurance rates fall 5% in Q3 2026." Global Insurance Market Index. October 21, 2026. https://www.marsh.com/en/corp/about/news/global-commercial-insurance-falls-5-percent-q3-2026.html.

[4] National Association of Insurance Commissioners. "2026 Report on the Cybersecurity Insurance Market." 2026. https://content.naic.org/sites/default/files/2026-report-cybersecurity-insurance-market.pdf.

[5] Hemenway, C. "NAIC report on the cyber insurance market." Insurance Journal, summarizing the NAIC 2026 report. October 27, 2026. https://www.insurancejournal.com/news/national/2026/10/27/890440.htm.

[6] Reinsurance News. "Coalition report finds sharp rise in ransomware demands as most businesses refuse to pay." Coverage of Coalition's 2026 Cyber Claims Report. 2026. https://www.reinsurancene.ws/coalition-report-finds-sharp-rise-in-ransomware-demands-as-most-businesses-refuse-to-pay/.

[7] Munich Re. "Global Cyber Risk and Insurance Survey 2026." April 2026. https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey-2026.html.

[8] Marsh. "Cyber resilience: Twelve key controls to strengthen your security." 2022. https://www.marsh.com/ca/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html.

[9] Marsh McLennan. "Groundbreaking Research from Marsh McLennan Reveals Direct Link between Key Cybersecurity Controls and Reduced Cyber Risk." Press release on "Using data to prioritize cybersecurity investments." April 6, 2023. https://www.marsh.com/en/corp/about/news/groundbreaking-research-from-marsh-mclennan-reveals-direct-link-.html.

[10] Global News. "Hamilton cyberattack cost." July 31, 2025. https://globalnews.ca/news/11313018/hamilton-cyberattack-cost/.

[11] Sebben, L. "Hamilton taxpayers on the hook for full $18.3M cyberattack repair bill after insurance claim denied." CTV News. July 31, 2025. https://www.ctvnews.ca/toronto/local/hamilton/article/hamilton-taxpayers-on-the-hook-for-full-183m-cyberattack-repair-bill-after-insurance-claim-denied/.

[12] Insurance Business. "Did Jaguar Land Rover's cyber insurance gap help pave the way to 4,000 job losses?" 2026. https://www.insurancebusinessmag.com/uk/news/cyber/did-jaguar-land-rovers-cyber-insurance-gap-help-pave-the-way-to-4000-job-losses-588902.aspx.

[13] The Register. "M&S pegs cyberattack cleanup costs." November 5, 2025. https://theregister.com/2025/11/05/ms_pegs_cyberattack_cleanup_costs/.

[14] Cybersecurity and Infrastructure Security Agency, MS-ISAC, NSA and FBI. "#StopRansomware Guide." 2023. https://www.cisa.gov/stopransomware/ransomware-guide.

[15] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." NIST CSWP 29. 2024. https://doi.org/10.6028/NIST.CSWP.29.

[16] TechTarget. "Coalition: Insurance claims for Cisco ASA users spiked in 2023." Coverage of Coalition's 2024 Cyber Claims Report. 2024. https://www.techtarget.com/cybersecurity/news/366582059/Coalition-Insurance-claims-for-Cisco-ASA-users-spiked-in-2023.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.