Shumaker

SEPTEMBER 29, 2026 | PUBLICATION

Client Alert: The Tightening Gate: How Cyber Insurance Carriers Are Raising the Bar on Conditions Precedent to Coverage

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Mark Lehman

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The cyber insurance market has evolved from a nascent specialty line into an evidence-driven discipline. Carriers that once underwrote cyber risk based on brief annual questionnaires now condition both the binding of coverage and the honoring of claims on specific, verifiable security controls, documented operational procedures, and ongoing compliance throughout the policy period. A single unimplemented control can support a coverage denial, trigger a policy limitation, or, where the carrier determines that an application representation was materially inaccurate, justify rescission of the policy.

A Rapidly Evolving Market

Demand for cyber coverage continues to accelerate even as underwriting grows more exacting. Global cyber insurance premiums reached an estimated $15 billion in 2025.[1] S&P Global Ratings projects that global premiums will continue to grow in the coming years.[2]

Ransomware continues to dominate the loss landscape. In the most recent reporting period, ransomware was present in 48 percent of confirmed breaches, representing a 44 percent increase over the year prior.[3]

While phishing was the leading cause of breaches, supply-chain compromises have risen significantly, and the global average cost of a data breach reached $4.99 million.[4]

Meanwhile, ransom payment rates have decreased. Chainalysis estimates that only 28 percent of ransomware victims made on-chain payments in 2025, a record low driven by law enforcement disruption and international coordination, improved resilience, and growing organizational reluctance to pay.[5] National Association of Insurance Commissioners (NAIC) data for 2024 show that of approximately 38,500 closed cyber claims, roughly three-quarters closed without a payout.[6] Carriers attribute a substantial share of non-payment outcomes to inadequate security controls, application misrepresentations, and untimely notice.

The New Non-Negotiables

The underwriting posture has shifted fundamentally. Carriers no longer accept general assurances of security readiness and instead demand continuous, documented proof of security control implementation. Carriers increasingly verify an applicant's external exposure and review records showing that relevant logs have been retained. The security controls below now routinely determine whether coverage will bind, whether carriers will offer favorable terms, and whether carriers will ultimately honor a claim. The overwhelming majority of cyber insurers condition coverage on some combination of the following:

- **Multi-Factor Authentication (MFA)** should cover remote access, email, and privileged accounts. Carriers increasingly regard text-message verification as inadequate and examine legacy environments, approved exceptions, and contractor pathways.
- **Endpoint Detection and Response (EDR)** should cover every managed endpoint. Carriers want to know who continuously watches the telemetry, how the organization contains a threat after detection, how personnel escalate an event, and whether the organization records the response.
- **Immutable and Offline Backups** should remain separated from storage that an attacker can reach because ransomware campaigns increasingly include backup infrastructure among their targets. Carriers often ask policyholders to perform recurring restoration tests and keep dated records showing that recovery succeeded.
- **Incident Response Plans** should address potential breach events. Carriers typically look for a current written plan that assigns escalation and notification steps. To maintain coverage, insurers may also ask policyholders to rehearse those steps in tabletop exercises at regular intervals.
- **External Vulnerability Scanning** gives carriers a view of internet-facing weaknesses before they bind or renew a policy. They may require the applicant or policyholder to close identified exposures, record the corrective steps, and retain the scan results.
- **Privileged Access Management (PAM)** should enforce least privilege through separate administrative accounts and controlled credential vaults. Carriers assess whether an organization removes unnecessary standing access and tracks activity involving sensitive systems.
- **Email Security (Domain-based Message Authentication, Reporting & Conformance [DMARC]/ DomainKeys Identified Mail [DKIM]/ Sender Policy Framework [SPF])** should inspect messages entering and leaving the organization and use authentication measures to limit spoofing and mailbox compromise. Carriers may verify that the organization has set its DMARC policy to quarantine or reject unauthorized messages.
- **Security Awareness Training** should reach every employee. Carriers frequently look for evidence of simulated phishing tests, a record of the instruction delivered, and proof that personnel completed it.
- **Network Segmentation** should divide the environment so an intruder cannot readily move between

systems, especially those holding sensitive data or supporting critical operations. Carriers examine whether the design would confine a compromise rather than allow it to spread throughout the environment.
- **Patch Management** should assign critical vulnerabilities a priority and a documented deadline for correction. Carriers review how promptly the organization deploys security fixes and how it records, prioritizes, and follows each item through closure.

Requirements vary by carrier, industry, and policy form. Some carriers accept a simple attestation, while surplus lines markets and high-limit towers increasingly request independent evidence, including external scans, penetration tests, or System and Organization Controls (SOC) 2 reports. Strong, documented security controls can reduce premiums, while applicants with material gaps may face rate increases, higher retentions, coverage exclusions, or outright declination. When an insurer requests information regarding an organization's security controls, corporate counsel and risk managers should provide accurate, verifiable information rather than describe the organization's aspirational security posture.

Consequences of Non-Satisfaction

Insurers now review cyber claims with heightened scrutiny, particularly regarding the security controls in place at the time of an incident. When an insured represents that it maintains specified security controls, policies, and procedures, any deviation from those representations can produce serious consequences, ranging from denial of the claim to rescission of the policy itself.

Travelers Prop. Cas. Co. of Am. v. Int'l Control Servs., Inc., No. 22-cv-2145 (C.D. Ill. Aug. 2022), illustrates the risk. In July 2022, Travelers Property Casualty Company of America (Travelers) asked a federal court to resolve its coverage obligations and rescind International Control Services, Inc's (ICS)s cyber liability policy. After a ransomware attack hit ICS in May 2022, the insurer reviewed an application that represented enterprise-wide MFA for remote access and administrative systems. The investigation found MFA on the firewall alone, while the other network assets had no MFA protection. The court granted the rescission of ICS's policy because the mismatch between the promised environment and the controls in operation constituted a material misrepresentation that affected Travelers' assessment of the risk.

A divergence between the security environment described in an insurance application and the security environment that existed at the time of an incident may give a carrier grounds to seek relief. Courts may permit claim denial or policy rescission on a misstatement in an application when the applicant acted negligently or in good faith, so long as the misstatement materially affected the risk.

Pre-Placement and Renewal Best Practices

Regulators, rating agencies, and carriers increasingly require affirmative treatment of cyber exposure. Policyholders should not rely on uncertainty in non-cyber policies but should instead confirm that dedicated cyber coverage addresses first-party loss, liability, vendor dependencies, and funds-transfer fraud. Policyholders should consider the following practices:

- **Conduct a Gap Analysis:** Before applying or renewing, inventory the systems and access paths that operate in practice, and compare that inventory with the carrier's requirements. Treat MFA, immutable and offline backups, and EDR as minimum controls. Examine remote access, email, cloud administration, legacy systems, and contractor accounts in addition to the primary office network.

- **Structure Application Representations Carefully:** An answer that overstates the organization's controls can place the policy at risk of rescission. Treat each response as a statement about the present state of a particular system. Have the person who manages that system verify the response, identify its scope and exceptions, and disclose any remediation plan instead of presenting a partial rollout as complete.
- **Preserve Documentation:** Keep dated versions of policies, control inventories, configuration reports, logs, testing results, training records, and approvals. Interstate Removal illustrates why an email trail by itself may not establish an "established and documented" verification procedure.
- **Match Policy Definitions to Actual Relationships:** Before binding, list the counterparties whose instructions employees may follow, including customers, vendors, lenders, clients, and payment intermediaries. A court may enforce those categories literally and reject a relationship that only the fraudulent transaction created or that a broader business setting merely implies.
- **Monitor Continuous Compliance:** Revalidate the controls whenever personnel changes, acquisitions, migrations, or new remote-access deployments alter the environment. Configure systems to flag disabled MFA, endpoints without protection, failed backups, and material configuration drift, and retain the records those checks produce.
- **Maintain Incident Response Readiness:** Because delayed notice can threaten coverage, give the response team decision rules, a reporting timetable, and current contact information. Assign responsibility for notifying the carrier, preserving evidence, retaining counsel, and coordinating the broker and breach-response vendors.
- **Document Remediation Efforts:** For each vulnerability, create a contemporaneous record that identifies the finding, evaluates the risk, notes interim safeguards, names the owner, sets a deadline, and includes proof of completion. That record can show that the organization used reasonable security measures and responded deliberately once it knew of the gap.

Conclusion

The tightening of conditions precedent in cyber insurance is structural, not cyclical. Carriers employ underwriting rigor, forensic evidence, and policy-specific control requirements to manage a volatile and expanding risk. For policyholders, cybersecurity investment now affects not only the likelihood of an incident, but also the availability and scope of risk transfer after an incident occurs.

Corporate counsel and risk managers should handle applications and renewals with the same care they bring to securities disclosures and regulatory filings. Corporate counsel and risk managers should make precise representations, preserve contemporaneous evidence, and maintain security controls rather than merely attest a security control's presumed existence and effectiveness.

Organizations that invest in enforced MFA, continuously monitored EDR, immutable backups, privileged access management, and documented incident response capabilities can improve both their security posture and their insurability. The tightening gate demands rigorous preparation, but it can align insurer requirements with practical reductions in cyber risk when policyholders implement, document, and sustain the controls they promise.

For further information or to discuss your individual circumstances, please contact Mark Lehman.*This article is for informational purposes only and does not constitute legal advice. Readers should consult qualified legal counsel regarding their specific circumstances.*

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

[2] S&P Global Ratings, Cyber Insurance Market Outlook 2026: Resilient Earnings, Tougher Competition, Pockets of Growth,
https://www.spglobal.com/ratings/en/regulatory/article/cyber-insurance-market-outlook-2026-resilient-earnings-tougher-competition-pockets-of-growth-s101658506

[3] Verizon, 2026 Data Breach Investigations Report,
https://www.verizon.com/business/resources/reports/dbir/ PDF:
https://www.verizon.com/business/resources/Td15/reports/2026-dbir-data-breach-investigations-report.pdf

[4] IBM, Cost of a Data Breach Report 2026,
https://www.ibm.com/downloads/documents/us-en/16dd90a741c46c2c

[5] Chainalysis, Crypto Ransomware: 2026 Crypto Crime Report 2026,
https://www.chainalysis.com/blog/crypto-ransomware-2026/

[6] Nat'l Ass'n of Ins. Comm'rs, 2025 Cybersecurity Insurance Report,
https://content.naic.org/sites/default/files/inline-files/2025_Cybersecurity_Insurance%20Report.pdf

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker