The New Cyber Insurance Reality: Exclusions, Requirements and What to Do About Them

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

The New Cyber Insurance Reality: Exclusions, Requirements and What to Do About Them

Cyber insurance is one of the most contested, litigated and misunderstood policies across all industries. Premiums continue to surge while coverage continues to narrow. Requirements remain a moving target and the fine print has become a masterclass in strategic ambiguity.

The problem is not that cyber insurance has become useless. On the contrary, it remains a critical component of enterprise risk management. The problem is that the growing gap between what business leaders believe their policy covers and what that policy will actually cover has never been wider. This guide examines the cyber insurance market as it stands in 2026: the exclusions carriers are leveraging to limit payouts, the security requirements now imposed as conditions of coverage, the threat landscape driving these shifts and strategic considerations organizations must act on to protect themselves.

What Your Policy Most Likely Won't Cover

In 2017, cyber claims rapidly expanded in frequency and severity. In response to that financial impact, carriers began a systematic and creative effort to rewrite what their policies specifically cover and more importantly, what they don't. Here are increasingly common exclusion and sublimit examples:

Act of War Exclusions

Perhaps no exclusion has generated more controversy than the act of war clause. When Merck & Co. was initially denied $1.4 billion in NotPetya-related claims by its insurer Lloyd's of London on the basis that the attack constituted an act of war by Russia, the industry sat up very straight and took note. Courts **ultimately sided with Merck in 2023**, but the message was clear: carriers would try. Since then, many policies have introduced "cyber war" and "state-sponsored attack" exclusions that are far more precisely worded and likely to be enforced.

Social Engineering Exclusions and Sublimits

Policies often limit or exclude claims relating to incidents that originate from social engineering, insider threats or business email compromise–three of the most common causes of incidents. This exclusion is a common concern and usually results in the purchase of additional coverage to specifically address these types of incidents.

Vendor Supply Chain Exclusions

Following the **CrowdStrike outage of July 2024**, which caused over $5 billion in losses across Fortune 500 companies, insurers began quietly adding language excluding losses stemming from widespread software failures, third-party platform outages and "systemic cyber events." If your business was crippled because a critical vendor's software update crashed global environments, you may find your policy points politely to the exit.

Ransomware Exclusions and Sublimits

Ransom payments and ransomware-related business interruption losses are increasingly subject to exclusions or sublimits, which are separate, lower caps than the overall policy limit. It is not uncommon to see a $10 million policy with a $1 million ransomware sublimit. Organizations that have not re-read their policies since renewal may discover this detail at precisely the wrong moment both reputationally and financially.

Negligence Exclusions

Carriers are increasingly denying claims where basic, industry-standard controls were demonstrably absent, such as unencrypted sensitive data. In practice, this means a carrier can argue that your loss resulted not from a covered cyber event but from your own negligence. If the claim is large enough, they may do so enthusiastically while citing nuanced exceptions to vague documentation from your intake or renewal questionnaire.

Underwriters once asked a handful of security questions on a one-page form, but now they conduct what looks far more like a technical audit of your entire security posture. Think of it less as applying for a policy and more as sitting for a cybersecurity examination, with your premiums determined by your grade.

What You Must be Prepared to Prove to Get Coverage

Lack of controls can result in declination, punitively high premiums or exclusions that hollow out your coverage. The following controls have become default requirements for obtaining meaningful coverage at reasonable premiums:

- **Continuous Monitoring:** 24/7 monitoring, ideally through a Managed Security Service Provider.
- **Endpoint Detection and Response:** Basic antivirus is no longer sufficient. Carriers want to see an industry-leading EDR solution deployed across 100% of managed systems.
- **Immutable, Segmented Backups:** Ransomware resilience is evaluated directly. Backups that could be encrypted alongside primary data provide no comfort to underwriters.
- **Internal Network Segmentation:** Preventing lateral movement between critical systems.
- **Multi-Factor Authentication (MFA):** Required across all privileged access accounts, email and remote access without exception. Carriers treating MFA as optional are non-existent.
- **Network Pentesting:** Conducting pentesting annually has become the floor rather than a ceiling. High-value sectors are now expected to conduct testing biannually or quarterly.
- **Privileged Access Management:** Controlling and auditing privileged account usage.
- **TableTop Exercises:** Annual live testing of Incident Response Plans.
- **Vendor and Third-Party Risk Management:** In an era of supply chain attacks, carriers want to see documented processes for assessing the security posture of critical vendors.
- **Vulnerability Management Programs:** Managing and remediating vulnerabilities through a robust program with defined service level agreements for critical and high findings.

The underwriting process has also lengthened considerably. Organizations should expect months, not weeks, for onboarding of meaningful coverage, with carriers requesting network scans, security questionnaires, financial statements and executive interviews. Renewal is not automatic and organizations that fail to demonstrate continuous improvement in their controls may find renewal terms significantly worse next year.

Beyond the Policy: Regulatory Risks That Can Compound Your Losses

Organizations must now navigate a thickening web of regulatory requirements. These three areas have the potential to compound losses well beyond what any policy will cover:

Ransomware Payment Sanctions Risk

OFAC guidance has made clear that paying ransom to sanctioned entities, or to groups operating on behalf of sanctioned nations, exposes organizations to significant civil and criminal liability, regardless of whether the payment was made in good faith. Many cyber policies now include language requiring pre-payment OFAC screening, and some carriers have explicitly excluded coverage for payments that trigger sanctions violations.

SEC Disclosure Requirements

The SEC's cybersecurity disclosure rules, fully in effect since late 2023, require public companies to disclose material cybersecurity incidents within four business days. This creates a direct tension with incident response best practices and with insurance claims. Carriers are watching public filings carefully and discrepancies between what companies report to regulators and what they report in claims can have serious consequences. Accurate, consistent incident documentation is no longer just good practice; it is a legal and financial necessity.

GDPR, CCPA and State Privacy Law Proliferation

Regulatory fines and penalties have historically been excluded from cyber insurance coverage in many jurisdictions. As US state privacy laws continue to proliferate, the potential fine exposure from a single breach has multiplied. Organizations must scrutinize whether their policies include regulatory defense costs and penalty coverage and in which jurisdictions.

Closing the Gap: Practical Steps for Stronger Cyber Insurance Outcomes

Cyber insurance in 2026 is not broken, but it is fundamentally different from what many organizations believe they have purchased. It remains a key component of strategic risk transfer, but the carriers have gotten smarter, the exclusions have gotten sharper and the requirements have gotten steeper. Organizations that treat their cyber policy as just a commodity purchase without active management are in effect, self-insured, they just do not know it yet. Here are five practical steps your organization can take to more actively manage and protect your coverage:

Annual Policy Gap Analysis

Leading organizations conduct a structured review of their policy against their current threat profile at least annually and following any significant change in their environments. This review should include legal and cybersecurity expertise.

Insurer Relationships, Not Just Transactions

The best outcomes at claim time consistently involve organizations that have cultivated relationships with their insurers and brokers before an incident. Carriers who know your security program, your team and your risk posture are significantly more likely to respond constructively when a claim is filed.

Layered Coverage Structures

Organizations with meaningful cyber risk exposure are increasingly working with brokers to structure layered programs that combine primary cyber coverage with excess layers, potentially from multiple carriers. This approach not only increases total available limits but reduces concentration risk.

Security Investment as Premium Management

Organizations often see investments in mature security controls translate directly into insurance premium reduction and coverage availability. The organizations paying the most for the least coverage are invariably the ones whose security programs are weakest. In this market, security spending and insurance spend are not separate line items, they are two levers on the same dial.

Board-Level Imperative

Cyber insurance should appear on the board risk agenda at least annually. Directors have a fiduciary responsibility to ensure that the organization's risk transfer strategy is aligned with its actual cyber risk exposure.

The good news is that the path forward is clear: invest in the controls that underwriters demand, read the exclusions that matter, build the relationships that smooth claims and review your coverage with the same rigor you would apply to any other material financial instrument. Cyber risk is not going away. Neither is cyber insurance. But only one of them is on your side, and only if you have done the work to keep it that way.

How Schneider Downs Can Help

Schneider Downs combines cybersecurity, risk management and industry expertise to help organizations address cyber insurance coverage challenges. Our approach aligns security controls with cyber insurance requirements and operational realities.

Through alignment with insurer expectations, always-on security controls and access to a trusted incident response partner, we help organizations like yours strengthen defenses, improve readiness and maintain a resilient cybersecurity posture against evolving threats and insurance scrutiny.

Ready to Get Started?

If you're interested in reviewing your policy exclusions, please contact our team at **cybersecurity@schneiderdowns.com** to schedule a cyber insurance gap analysis with one of our cybersecurity experts.

About Schneider Downs Cybersecurity

The Schneider Downs Cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our Digital Forensics and Incident Response teams are available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

For more information, please contact our team at **cybersecurity@schneiderdowns.com** or visit **www.schneiderdowns.com/cybersecurity**.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX
AUDIT AND ASSURANCE
CONSULTING
WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

METROPOLITAN WASHINGTON
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003