# TOP 5 REASONS CYBER LIABILITY INSURANCE COMPANIES DENY CLAIMS

With an alarming uptick in data breaches and ransomware in recent years, an increasing number of businesses have opted to add cyber risk insurance to protect themselves from catastrophic loss.

However, as the threat landscape continues to expand, many insurance companies are restricting payouts by creating more claim exceptions and exclusions. While some of these are clearly stated, others are hidden within confusing policy applications. This leaves many policyholders holding the short end of the stick when the insurer looks to disqualify a claim.

With ransomware claims skyrocketing, some insurance providers have introduced endorsements for Neglected Software Vulnerabilities. These endorsements apply a sliding scale of diminishing coverage if a known vulnerability is exploited while a patch was available but not applied.

**Here are the five most common reasons cyber liability companies deny claims:**

### 1 COMPANIES HAVE POOR PREVENTION PRACTICES IN PLACE

The number one reason insurance companies deny claims is because clients fail to comply with insurance policy practices to secure data. For example, some providers require you to install security software programs and regularly check your network for security threats. Others mandate that you change your passwords regularly, access your databases through a secure server and take other security precautions. Review your policy carefully to understand what's required.

### 2 COMPANIES FAIL TO DOCUMENT PREVENTATIVE MEASURES

The key to ensuring insurance payouts is documentation before disaster strikes. Delivering reports that show due care to maintain a secure environment is one way to help you get paid. To avoid any hassles, be sure to have accurate and updated documentation at all times.

### 3 EXCLUSIONS IN COVERAGE

Policies are increasingly scrutinized and may exclude certain types of attacks, such as insider threats or state-sponsored attacks. Depending on the perpetrator, insurers may cite a "war exclusion" clause on attacks by nation-state actors. Issues stemming from pre-existing vulnerabilities or breach conditions that existed before the policy was purchased are often excluded.

### 4 ACCIDENTAL ERRORS AND OMISSIONS

Building out bulletproof evidence in your favor ahead of time will help you make an undeniable claim for maximum payout. Reporting, coupled with detailed compliance, is essential in recuperating costs from an attack. The documented evidence should include everything you have done to abide by the terms put forth by the insurer.

### 5 COVERAGE DOESN'T EXTEND BEYOND INTERRUPTION TIMEFRAME

Liability insurance plans vary. You should pay close attention to coverage timeframes. It could mean the difference between covering all your losses versus just a small percentage.

Both ransomware attacks and ransomware insurance coverage are on the rise. Unfortunately,companies with ransomware coverage are finding that cyber policies are not always the silver bullet they expected.

**TIP:**

***Many cyber insurance providers have their own incident response teams and approved vendors for forensic investigations. It's important to understand your insurer's incident response requirements before finalizing your policy.***

**If you want to learn more about how Unitrends Unified BCDR provides a complete and agile solution to eliminate ransomware and downtime**

**GET A DEMO TODAY**

## ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

16122024