



## INSURANCE BUYERS: BEWARE OF FAULTY CYBER CRIME POLICIES

An insurance pro points out the potential pitfalls in policies that ‘insureds’ might overlook

By *Anto Almasian*

If you think all cyber insurance policies are the same, think again!

What may surprise you is that, unlike many other insurance policies you purchase, cyber policies don’t share any common policy forms. Each carrier custom tailors their insuring agreements that make up your policy. Technically, this is referred to as a “Named Perils” policy. The coverage only applies to what’s explicitly stated in the policy.

So why is this important? Many policyholders believe that when shopping for cyber insurance, as long as the limits match, the process is apples to apples. Unfortunately, that’s not the case. Policyholders (aka “insureds”) need to be hyper-aware that depending on the policy, coverage can change.

For example, cyber crime is often a reason for insureds to purchase coverage. Stories of wire transfer fraud and ransomware are rampant for a good reason. According to the law firm BakerHostetler’s 2023 Data Security Incident Response Report ([bit.ly/BakerHReport](https://bit.ly/BakerHReport)), the current year has experienced dramatically increased ransomware activity compared to 2022. Their research also has shown that ransomware accounts for 28% of all cyber incidents, with an average ransom payment of over \$600,000 and significantly longer recovery times than in years past. Wire Transfer Fraud wasn’t far behind, accounting for 13% of incidents, with a median wire transfer loss of \$97,044 and funds recovery on only 24% of all cases.

As you can see, buying protection is critical for all businesses. Using those two coverages as examples, let’s look at

how coverage can vary from policy to policy...

### CARRIER A

- **WIRE TRANSFER FRAUD**—Covered under the Funds Transfer Fraud insuring agreement. The agreement provides clear limits and definitions of coverage.
- **RANSOMWARE**—Covered under the Extortion insuring agreement at full policy limits. Again, the language is easy to read and clearly explains the coverage circumstances.

### CARRIER B

- **WIRE TRANSFER FRAUD**—Covered under the Computer and Funds Transfer Fraud insuring agreement. Only provides wire transfer fraud coverage if the fraudulent instructions are written.
- **RANSOMWARE**—Covered under the Extortion insuring agreement but is sublimited to 5% of the policy limits or 50%, depending on your internal controls.

### CARRIER C

- **WIRE TRANSFER FRAUD**—Covered under the Fraudulent Impersonation insuring agreement. This agreement only covers wire transfer fraud if a pre-arranged callback or other policies were used to verify all transfer instructions.
- **RANSOMWARE**—Covered under Computer Attack and Cyber Extortion insuring agreement, but when investigated further, the coverage is reduced to 10% limits available for forensic investigation, negotiation and ransom payment. The other 90% is available for media relations and loss of business.

As you can see, the lack of consistency in the cyber insurance industry can confuse insureds and make it challenging


to compare policies and quotes. In a real-life example, look no further than the court case of *New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London*. In this case, the New Hotel Monteleone LLC bought a cyber policy with an aggregate limit of \$2 million. However, when a data breach occurred, coverage for the loss they suffered was sublimited to \$200,000. This was a surprise to the New Hotel Monteleone management. They were under the impression that they had \$2 million for the incident. This confusion in limits actually led to a lawsuit filed against Lloyd's by New Hotel Monteleone. Eventually, New Hotel Monteleone dropped the lawsuit, presumably, because the limits and language in the policy were clear as to the limitations of coverage.

**BOTTOM LINE? DON'T MAKE THE MISTAKE OF THINKING THAT ALL CYBER INSURANCE COVERAGE IS THE SAME. AT EACH RENEWAL AND AT ALL ALTERNATIVE POLICY PROPOSALS, YOU SHOULD HAVE A FULL COMPARISON PROVIDED TO YOU WITH CLAIMS EXAMPLES OF HOW EACH SUBLIMIT AND INSURING AGREEMENT WOULD WORK.**

Bottom line? Don't make the mistake of thinking that all cyber insurance coverage is the same. At each renewal and at all alternative policy proposals, you should have a full comparison provided to you with claims examples of how each sublimit and insuring agreement would work. Without a clear comparison of what you have vs. what the carrier is proposing, it's very difficult for businesses to make an educated decision on coverage.

If you'd like a fresh set of eyes to review your policy options, or offer an alternative quote, please don't hesitate to reach out to me using the information below.



 **ANTO ALMASIAN** is a risk management consultant affiliated with Haylor, Freyer and Coon an Alera Group Company, Syracuse, NY. Contact him at [aalmasian@haylor.com](mailto:aalmasian@haylor.com) or call 315.703.1387.

# REDUCE. REUSE. RECYCLE.



Reduce



With Uptime Intelligent Machine Manager can shrink downtime and eliminate common hassles.

Reuse



With Ludell Heat Recovery Systems to save on fuel consumption and minimize steam requirements.

Recycle



With Nautilus™ 2.0 ceramic filler membrane system designed to diminish overall operating costs.

**SPEAK WITH AN ELLIS WATER SOLUTIONS EXPERT**

**PARTNER WITH INNOVATION**