NFP
An Aon Company

Property and Casualty
General

Silent Cyber Days Are Ending

Why Cyber Insurance Can't Be Considered Optional

Chris Krako, Vice President, Claims Advocacy | Management, Cyber and Professional Liability

Many businesses naively believe that the coverage afforded them through their general liability and property policies will protect them in more scenarios than is accurate.

One such belief is that coverage can be captured under these policies for a cyber loss. While we have seen policies respond to cyber claims under "silent cyber" coverage, regulatory changes and exclusionary language in general liability or property policies means that those who count on these policies to cover a cyber event may find themselves in for a costly surprise.

What Is Silent Cyber?

Silent cyber, also known as non-affirmative coverage, occurs when the language in a policy that dictates coverage is vague or "silent" regarding a specific type of loss. In this case, when policy provisions do not explicitly mention or preclude cyber loss, it can lead to confrontations over coverage between the policyholder and insurer. Often this means expensive and protracted litigation finalized by a court determination as to the application of coverage. These types of disputes underscore the importance of understanding silent cyber risk and how it may impact your business.

Commercial Coverage

Commercial policies like commercial general liability, commercial property and business owner's policies are not designed to cover the expenses and damages incurred due to a cyber event. While under certain situations we have seen silent cyber coverage respond, often that coverage is limited or woefully inadequate for the loss incurred. Businesses must consider their broader cyber exposure when evaluating whether they're truly protected.

Regulatory changes and exclusionary policy language are eliminating "silent cyber" coverage. If a cyber event occurs at your business, will you have the coverage you need to address it?

Incidents Occur: Breaches, Malware, Ransoms and More

The response services that a cyber breach requires – breach counsel, forensic IT, data recovery, notification communications and crisis management – can add up fast. These first-party expenses are excluded under a liability policy, and while some property policies may provide response costs, they are extremely limited and would cover a small fraction of accrued costs in the aftermath of a cyber or privacy breach.

Malware can be introduced into electronic equipment, rendering them inoperable and irreparable (an event known as bricking). Property policies are unlikely to cover the replacement of the equipment as there is no direct physical loss or property damage despite the equipment being unusable.

Even kidnap and ransom policies, which are designed to respond to ransom claims, will exclude any extortion or ransom arising from a cyber event, ensuring they are not going to cover a ransomware claim. These are just a few silent cyber examples that reveal how risky it can be to rely solely on general policies.

Industry Trends

Silent cyber coverage is rapidly declining due to regulatory actions, underwriting practices and court decisions:

Lloyd's Directive: Lloyd's of London required all policies to clearly affirm or exclude cyber coverage by January 2020 (**Lloyds Market Bulletin Y5258**).

ISO Changes: In 2020, ISO mandated endorsements excluding cyber events from commercial property policies (**ISO Cyber Incident Exclusion - Commercial Property Form**).

Legal Precedent: An appellate court ruling in January 2025 determined that a very popular home goods and improvement chain's general liability policies did not cover losses from a 2014 data breach. Despite having cyber insurance, coverage was insufficient, forcing the company to pay nearly half of a $170 million settlement (thus, out of pocket.)

Regulatory Action (UK): In January 2019, the Prudential Regulation Authority instructed insurers to explicitly address cyber risks (**Anna Sweeney Letter**).

Get a Comprehensive Cyber Policy

Cyber threats are no longer rare. From ransomware attacks to data breaches, today's threats demand more than a patchwork of outdated protections.

A comprehensive cyber policy helps you proactively respond to evolving threats. It connects you with breach coaches, forensic IT teams and crisis communication experts the moment something goes wrong. It covers business interruption losses, reimburses ransom payments and helps recover your data to minimize disruption and speed up recovery.

Our cyber experts at NFP can help protect you. You've worked hard to build your business — now work smart to keep it safe with a well-structured cyber policy that supports long-term cyber exposure management.

For your business.
For your people.
For your life.

NFP.com

NFP®
An Aon Company