expert.ai

How Cyber Insurance Has Evolved in 2021

Expert IQ Report

The insurance industry is undergoing unprecedented change to remain relevant in a risk environment that is evolving even faster as result of the pandemic. According to **recent research**, global cyber-attacks increased by nearly a third in the first half of 2021. And not only did ransomware incidents jump 93%, but the average ransom demand also increased an astounding 518%, while actual payments rose more than 80%.

As a result, **cyber insurance** has become especially critical for many companies. Yet, the volume of attacks and their success has caused the price of coverage to climb dramatically, and in general, confusion reigns.

The following Expert IQ Report has been developed by expert.ai using **expert.ai natural language understanding** (NLU) to analyze a sample of approximately 1,130 articles published between January 2021 and November 2021 by a range of industry outlets (e.g., Insurance Insights, Insurance Business Magazine US/UK/CA, Risk & Insurance, Insurance Age etc.) focused on insurance news, opinions and analysis.

Our goal was to identify how cyber insurance has evolved throughout 2021 in a context where, according to **Hiscox Cyber Readiness Report 2021**, "Adoption of cyber insurance is creeping up — both through standalone policies (27% now have one, up from 26%) or another policy (34% compared with 32% last year.)"

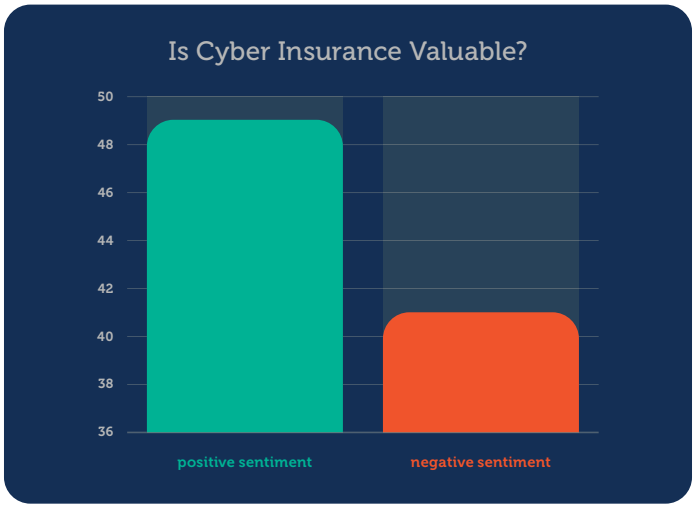
Products and Policies

Many studies highlighted the emergence of cyber insurance in the last couple of years. Pandemic lockdowns accelerated the digitalization of business processes and the adoption of remote working practices became the norm. However, the rush to get workers online and lax home security has created greater cyber vulnerabilities. With cyber insurance in the spotlight, many predicted a corresponding increase in spend by enterprise businesses on cyber insurance in 2021. And, in fact, this would turn out to be the case as infosec experts and vendors alike have reported **premiums increasing upwards of 50%** — some closer to the 100% mark.

From the sample of analyzed articles, 18% were found to be related to the cyber landscape. Cybersecurity and cyber risks were common themes in insurance realm for both the need to design suitable cyber products (57%) as well as the potential impact on existing contracts (36%).

Defining the Market

Looking at the overall sentiment of articles correlated to the cyber insurance market value (more than 14% articles out of the 1,130 analyzed), cyber insurance is being discussed in a more slightly positive light than negative. However, this might seem a countertrend according to some industry analysts. According to market research firm **Forrester**, "Insurers have been collecting small premiums while facing near infinite risks. At least one top-10 cyber insurance carrier will cease writing new business and selectively run off existing business in 2022."



However, the need for regulations within the cyber insurance market (10% of articles) is seen as a negative.

Are Insurers Aware of Cyber Risks to Which They Are Exposed?

According to our sample analysis, more than 19% of articles show a correlation between cyber and the COVID-19 pandemic. This seems to prove that underwriters are struggling to evaluate the cyber exposure correlated to pandemic-generated vulnerabilities. In addition, 2.9% of cyber articles (205 articles out of the 1,130 analyzed by expert.ai) are related to silent cyber which refers to cyber risks that are neither explicitly covered nor excluded in policies.

In fact, unlike cyber insurance that clearly defines the parameters of cyber coverage, traditional policies such as property and casualty do not. The latter are those most likely to result in litigation or unintended exposure. If there is no explicit cyber exclusion in a policy, insurers may be liable to cover losses caused by cyber perils. The potential for aggregated loss from these underlying exposures is currently one of the major issues being considered by the insurance/reinsurance industry.

Lloyd's of London required all syndicates to provide clarity on the cyber exposure in all their policies, giving clients contract certainty. **This approach started in 2020** and has been phased in over the course of 2021. It particularly aimed at eradicating silent cyber from traditional lines of insurance by encouraging insurers to identify the exposure and either clearly exclude or affirmatively include it. The same approach can be seen by regulators, including the European Insurance and Occupational Pensions Authority and the National Association of Insurance Commissioners in the United States, who have issued guidelines to help firms manage this risk.

Is Cyber Insurance Fostering Cyber Resilience?

In the last few years, evolving cyber risks have been plaguing organizations and testing their resiliency. Cyber resilience refers to an organization's ability to prepare for, respond to, and recover from cyberattacks and data breaches while continuing to operate effectively.

Resilience emerges as the main topic across 67% of cyber-related articles analyzed by expert.ai, proving that the **insurance sector is still relevant to the global improvement in cyber resilience** despite the complexity of effective risk analyses, the ambiguity of policies coverage and lack of historical data.

Expert IQ Report

Produced using expert.ai natural language understanding (NLU) capabilities, the Expert IQ Report is a series that looks to provide deep content analysis of the massive amounts of language data on a given event, person or topic. Expert IQ Reports demonstrate the value of using AI-based NLU technology to automatically generate a fast and accurate understanding of language data.

https://www.expert.ai