Average insurance gap after cyber events is 350%, research finds

By Erin Ayers, Front Page News

Just 20% of companies carried adequate cyber insurance to fully cover their financial losses after data breaches, with an average protection gap of 350%, according to research from CYE.

A coverage gap of 350% leaves more than 75% of incidents uninsured, for an average uncovered loss of $27.3 million, CYE found in its analysis of 101 cyber events across several industries. More than 35% of companies studied experienced a gap of more than 100%. In extreme cases (about 7%), the coverage gap reached nearly 3,000%.

The finance/insurance and education sectors were found to have the largest coverage gaps, which CYE attributed in part to these industries' heavy reliance on digital systems to function. The report also revealed smaller businesses with less than $10 million in revenue are more likely to be underinsured.

"In cases of bootstrapped companies, with no large investments backing them, an uncovered breach can be a death blow that effectively ends company operations," said CYE in the report. "These types of companies should exercise extreme caution with their cybersecurity hygiene or make sure they have sufficient coverage."

There are a few reasons companies may face a protection gap. CYE reported. In some cases, companies couldn't buy as much cyber insurance coverage as they wanted or fell short in accurately quantifying their own cyber risks. In others, claims weren't fully covered by the companies' insurance policies.

The report offers a few examples, including a 2019 cyber event at Orrstown Bank involving a dispute between the bank and its insurer. A partial claim denial left the bank with coverage for just $486,000 of its $765,000 financial losses.

Another bank breach in 2019, affecting Capital One, resulted in losses of $138 million. Though the financial giant's insurers paid out $73 million for the claim, it still had to shoulder $65 million in uninsured losses.

CYE also examined the December 2020 SolarWinds cyber incident, which resulted in an estimated $126 million through September 2023. Insurance has covered about $66 million, according to the report.

"SolarWinds bore a substantial financial burden due to the cyber incident, reflecting the challenge of fully compensating for such breaches through insurance alone," CYE said.

The coverage gap also hasn’t declined in recent years, the firm noted, suggesting the problem has gotten worse.

“The findings underscore a pressing need for businesses to refine their approaches to cyber risk quantification,” commented CYE. “The prevailing underestimation of cyber risks leads to insufficient coverage, exposing companies to substantial financial vulnerabilities post-breach. Companies need to remember that insurance companies can’t (or won’t) cover very high risks [and] covered risks almost never account for business risks like churn and loss of business continuity.”