Published on *The National Law Review* https://natlawreview.com

Don't Panic-Buy Your Cyber Policy: Evaluating New Approaches to Cyber Risk

Article By:

Vincent E. Morgan

Claire E. Cahoon

Panic-buying made a post-pandemic comeback when a critical channel for gasoline, diesel, and jet-fuel was forced shut down in the wake of a ransomware attack. Suddenly, gas became the new toilet paper: a treasured commodity. Upticks in devastating ransomware attacks, like the one that crippled pipeline operations and led the victim to pay a $4.4 million ransom, are shaking up the cyber insurance market, where comprehensive coverage is becoming increasingly in-demand and hard-to-find.

Cyber insurance policies typically cover several types of losses incurred in a cyber-attack. Depending on the policy, some cover ransomware payments. But as ransomware attacks grow in number and heft, the market is shifting. Policyholders are seeing insurers changing policy terms and coverage as the frequency and severity of ransomware attacks increase.

Insurers that cover ransomware payments are becoming increasingly worried that these developments will lead to unsustainable losses. Roughly six weeks before the pipeline cyber-attack, CNA Financial Corp., one of the world's largest insurance companies, paid $40 million to recover its IT network from cybercriminals. Though many businesses do not disclose ransom payments, the $40 million payout is the highest reported ransom in history. REvil hackers hoped to set a new record, recently asking the victims of its latest ransomware attack to cough up $70 million.

The low cost and high profitability of committing ransomware attacks is feeding further activity. In April, the Justice Department reported that "by any measure, 2020 was the worst year ever when it [came] to ransomware and related extortion events." According to Palo Alto Networks, the average ransomware attack payment in 2020 was $312,493.00, a 171% increase over the previous year. As Tufts cybersecurity policy professor Josephine Wolff said, "one of these incidents spurs so many claims that insurers start feeling like, 'We're not going to be able to cover all of these. There were too many people affected. It was too expensive. We need to not be on the hook for all of this."

Simultaneously, the looming threat of ransomware attacks also heightens demand for cyber insurance across all industries. In the Cyber Insurance Report published by the Government Accountability Office (GAO), more than 60% of brokers surveyed reported that "the top two drivers of

new or increased sales of cyber insurance were clients experiencing a cyber-attack or hearing that others suffered from an attack."

But as more businesses seek coverage for cyber incidents, the insurance industry is still working with limited knowledge on the frequency and severity of attacks, which can lead to inconsistent risk assessments and, thus, policy rates and limits. Most cyber-attacks go unreported or undetected, and the lack of a centralized source of information about cyber events limits the data needed for comprehensive actuarial evaluations. In other lines, insurance companies rely on historical loss data to determine risk and premium rates. That same approach is harder due to incomplete data, and while the industry is taking steps to close this information gap, policyholders will likely continue to see inconsistencies in cyber coverage.

Other potential challenges include:

- businesses' narrow awareness of issues;
- affordability for small and mid-sized companies;
- the risk of aggregated losses from a cyber-attack; and
- insurers placing specific limits on ransomware coverage, adding exclusions to traditional lines of coverage, and tightening policy terms and conditions, particularly in risky sectors, like health care, education, and public entities.

As the cyber insurance industry grapples with both uncertainties and complexities, policyholders will almost certainly see changes to their cyber policies. Bracewell attorneys are ready to help policyholders navigate the cyber-insurance evolution. Cyber risks are perhaps some of the greatest risks businesses face today, and policyholders should seek protection where they can. Taking proactive steps instead of panic-buying in the wake of an attack could avoid the waste of premium dollars and allow for better protection.

Abby Lahvis, a Bracewell LLP summer associate, also contributed to this article.

© 2025 Bracewell LLP

National Law Review, Volume XI, Number 208

Source URL:https://natlawreview.com/article/don-t-panic-buy-your-cyber-policy-evaluating-new-approaches-to-cyber-risk