Cyber-attack insurance is a complicated necessity

By Martin Potgieter

11 Oct 2023

They say death and taxes are inescapable, but we can add another certainty to that list: the escalating number of cyber incidents threatening the financial health of businesses. This isn't the surge in attacks; it's also about the rising premiums that cyber insurance companies are demanding. It's a double whammy for organisations, as the menace of cyber intrusions intensifies and the cost of safeguarding against them soars.

The Council of Insurance Agents and Brokers (CIAB) recently disclosed statistics showing a roughly 28% increase in cyber insurance premiums in the first half of 2022 compared to the same period in 2021.

By 2022's end, premiums had climbed an additional 20.3% over the previous year. These figures align with data from Statista, which revealed that 89% of insurance brokers observed a heightened demand for cyber insurance policies during the same timeframe, and 72% reported an uptick in claims.

ECOM Africa transforms into Converge Africa

1 Sep 2023

As cyber insurance claims went up, insurance companies began putting stricter limitations on what they cover and what businesses must do to keep their coverage intact. It's all because of the ever-growing complexity of the cybersecurity landscape.

These insurance providers prioritise their own protection by demanding that their customers put certain levels of security in place. As a result, there has been a major clamp-down on what type of coverage these companies provide and what they expect their customers to do to ensure the insurance remains valid.

The consequences of paying

An important question to consider is: How much does cyber insurance influence attacker behaviour? Payouts made to these criminals have not only changed the way they target and demand ransoms, but it has also become a tempting reward

for them.

However, it's worth noting that some cyber insurance policies have started excluding ransom payments from their coverage. This means that organisations relying solely on insurance may no longer have the guarantee of ransom payment if they fall victim to a cyberattack. This shift in policy coverage aims to discourage attackers from targeting organisations with the expectation of a payout.

Cyber insurance is no longer something that offers peace of mind and allows the organisation to relax. Instead, it has become a last-resort protection that comes into play when all other measures have failed – but only if the policy explicitly covers ransom payments. The game has changed, and both companies and insurers need to navigate this new reality with caution.

Cyber insurance alone is not enough

While cyber insurance is important and should be a priority for the C-suite, it's not foolproof. The threat landscape can be challenging. Ransomware payouts have skyrocketed in recent years, emboldening attackers. They're now using double and triple extortion to increase their profit margins.

They encrypt the data, demand the ransom, and then start going to your business partners and telling them that your company has been compromised and that their data is now also at risk. They threaten to release your partner's information alongside your own and demand money from everyone involved. Cyber-insurance can't protect against this level of reputational threat.

That is why cyber insurance companies are now telling their customers what to do to ensure their insurance stays valid. Companies are now under pressure from multiple fronts — regulation, attackers, and insurers — to guarantee that every security step is taken should they be compromised.

Companies need to reinforce their security systems and investments and collaborate with third-party service providers to ensure comprehensive protection.

ABOUT THE AUTHOR

Martin Potgieter is a technical director and solutions-focused cybersecurity specialist, and cofounder of Nclose