Does Your Cyber Insurance Policy Look More Like Health Insurance?

Blog Workplace Privacy, Data Management & Security Report

Jackson Lewis PC

USA | January 3 2022

Over the past several years, if your organization experienced a cyberattack, such as ransomware or a diversion of funds due to a business email compromise (BEC), and you had cyber insurance, you likely were very thankful. However, if you are renewing that policy (or in the cyber insurance market for the first time), you are probably looking at much steeper rates, higher deductibles, and even co-insurance, compared to just a year or two ago. This is dependent on finding a carrier to provide competitive terms, although there are some steps organizations can take to improve insurability.

What's going on?

The short answer is what one might expect, claims paid under cyber insurance policies are significantly up, according to Marc Schein*, CIC, CLCS, National Co-Chair Cyber Center of Excellence for Marsh McLennan Agency who closely tracks cyber insurance trends. Mr. Schein identified the key drivers hardening the cyber insurance market: ransomware and business interruption.

- **Ransomware**: According to FBI data, adjusted losses from ransomware matters tripled from 2019 to 2020. Further, according to an Allianz Global Corporate & Specialty (AGCS) cyber insights report, cited in Insurance Journal, the U.S. experienced a 62% increase in ransomware incidents during the first six months of 2021 and a 225% increase in ransom demands.
- **Business interruption**: Business interruption costs following a ransomware attack more than doubled over the past year, increasing from $761,106 to $1.85 million in 2021, with down time averaging 23 days, according to the same AGCS report.

According to Fitch Ratings' Cyber Report 2020, insurance direct written premiums for the property and casualty industry Increased 22% last year to over $2.7 billion, representing the demand for cyber coverage. The industry statutory direct loss plus defense and cost containment (DCC) ratio for standalone cyber insurance rose sharply in 2020 to 73% compared with an average of 42% for the previous five years (2015-2019). The average paid loss for a closed standalone cyber claim moved to $358,000 in 2020 from $145,000 in 2019.

The effects of these, other increases in claims, and losses from cyberattacks had a dramatic impact on cyber insurance.

- Rate increases of 100% to 300% are not uncommon. According to Marsh's November Cyber Market Report, the average U.S. cyber price per million in coverage increased 174% for the total price per million for the 12 month period ending September 2021.
- Capacity has decreased dramatically, with $10 million limits becoming challenging to secure.
- Policy changes, such as increases in deductibles, retention, sublimits, and co-insurance on ransomware payments, are making cyber coverage look more like health insurance.

What can we do?

Perhaps the most concerning development for organizations in the cyber insurance market is the significantly increased scrutiny carriers are applying to an applicant's insurability. The days of the three-question application process may be over. According to Mr. Schein, before applicants look to procure cyber coverage, an astute buyer should contemplate the following underwriting cyber security controls. Examples of these include:

- Multi-factor authentication across the applicant's systems including for email, remote access, vendor access, etc.
- Adoption of a tested incident response plan.
- Presence of an endpoint detection solution.
- Security awareness training, including phishing training.
- Removing end-of-life software.
- Closed remote access ports, including remote desktop protocol (RDP).

This is consistent with Mr. Schein's experience with organizations anxious to bolster information security controls in connection with the underwriting process for cyber insurance. The controls mentioned above are typically best practices underwriters are strongly encouraging which may also improve an organization's compliance posture. Notably, they are not limited to technical IT fixes, but include broader administrative policies and practices, such as training and breach preparedness.

Indeed, an increasing number of states require businesses to implement "reasonable safeguards" to protect personal information. In New York, for example, the New York SHIELD Act requires businesses of all sizes to adopt administrative, physical, and technical safeguards to protect the personal information they maintain about New York residents. The statute does not require specific technical safeguards be maintained. The California Privacy Rights Act (CPRA) adds to the California Consumer Privacy Act (CCPA) an affirmative obligation to "implement reasonable security procedures and practices…to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." Considering what IT experts have been saying about the effectiveness of multifactor authentication, it has been identified as a meaningful control albeit not full-proof tool to help prevent unauthorized access to information systems within the scope of privacy and security regulation.

Of course, there are no silver bullets, but such safeguards may dramatically reduce the chances of a cyberattack, and that is music to an underwriter's ears. There will be claims, just fewer of them, and perhaps less damaging.

Jackson Lewis PC - Joseph J. Lazzarotti and Marc Schein