CYBERATTACKS
A Worsening Threat & Resulting Impact on the Insurance Market

If one thing hasn't slowed down as a result of the upending of the world in the last couple of years, it is cyber threats. In fact, they have increased across the board. The threats and their related services are higher interlinked. Business interruption insurance, the pandemic, and cyber threats combine to demonstrate one of the largest vulnerabilities the modern, more connected world has to face. Security protocols to defend against cyber threats have not caught up with the advancing technology and rapidly changing workplace, and being caught off guard in that way has led many companies to face huge losses.

The way business has changed over the last couple of decades has led to an increasing reliance on outside parties for data management and a slew of other services through SaaS (software as a service) companies. Unfortunately, changing from in-house solutions to outside vendors for many of these enterprise services and applications has led to lax security protocols. Often, these companies do not update response plans for events like cyberattacks and often do not have adequate offsite backups of their data.

Cyber criminals, in turn, have begun taking advantage of holes in security. The weakest link in any security plan is often the humans who must implement it, and switching to remote work and working from home, sometimes on personal electronic devices, is much harder to monitor, secure, and test. According to a report from the United States Government Accountability Office (GAO), the number of clients seeking cyber threat mitigation and cyber insurance has **doubled between 2016 and 2020**. What has become a benefit to brokers and agents is rapidly becoming a risk for the insurers they utilize.

During 2020 and 2021 alone, cyberattacks of all types on organizations of all sizes have increased steeply, especially when it comes to ransomware. Those attacks have led to a similar increase in claims and have placed a huge strain on carriers' portfolios. What is the result? There has been an uptick in tension between agents and carriers, and insurers have increased premiums and changed the practices they use for underwriting. They have also become wary of insuring aggregated portfolios.

AHT INSURANCE
A BALDWIN RISK PARTNER

THE INDUSTRY BEING REALISTIC

It is tempting to look on the bright side, and there are absolutely positives coming out of the pandemic and the way businesses are beginning to look at cyber threats. With that being said, it doesn't pay to look on the bright side and ignore negative aspects of the situation. Attacks are rapidly becoming more sophisticated, companies are becoming more inclined to pay for their data in the events of ransomware attacks, and the current geopolitical climate is rapidly becoming very beneficial to cyber criminals.

Losses are building and building for carriers as a result of increasing numbers of attacks on their cyber infrastructure. Those losses have led them to be more wary about the situations they will cover, what new clients they may take on, and to take a more conservative stance, in general, in relation to cyber security. Many cyber insurers rely heavily on reinsurers, leading to roughly half of their own cyber premiums heading to the reinsurance market, with 60% landing in the hands of just four reinsurers.

Why are the recent upticks in cyber threats seemingly catching these companies off guard? They cite a lack of cyber-loss data as a major cause due to a lack of historical precedent. The insurance industry is the foremost authority in actuarial sciences and should have been building large repositories of data regarding claims, policies, and threats over the last two decades. As a new area of risk, cyber threats represent a need for understanding that could have been resolved through the study of statistics and probability, both of which the industry should have known it would need as an informed basis for underwriting. Unfortunately, instead of doing the work to compile those issues, many companies chose to, instead, aim for the highest market share and grab their piece of the metaphorical pie before doing the back-end work to ensure everything was being done properly.

THE OTHER SIDE OF THE COIN

Compounding that risk from the insurance industry itself is the issue of companies who need to be insured. Often, they do not have a firm understanding of their risks. Many companies utilize simple formulas to determine how much risk they may face, such as multiplying the number of records and data points they have by a single figure to estimate their coverage needs.

The reality is that the only way for companies to accurately determine their potential losses from cyberattacks is through a thorough assessment. That cyber security assessment would include an analysis of the operations, the technical environment, the financial data, and the compliance requirements of the company. That process is relatively straightforward for small and mid-sized companies, but it becomes both more challenging and dramatically more complicated for larger companies with $1 billion in revenue or more.

Ultimately, most companies should turn to professionals, either within the insurance companies they are working with or through cyber industry professionals who can help determine their risks and establish a strategy moving forward that is in alignment with best practices and standards.

The risks of allowing cyber threats to loom without addressing them is so high from a monetary and regulatory standpoint that it is simply unacceptable to let them stand without doing anything.

Talk to us about your cyber risk mitigation strategy.

Prepared for BRP's Middle Market firms by Gwen Luu of JGS Insurance - a BRP Partner