RT ProExec
INSIGHTS
VOLUME XXII ISSUE 1 WINTER 2021

CYBER INSURANCE: A HARDENING MARKET

Cyber Insurance is still considered a relatively new insurance product. In the early days of the coverage, many insurers entered the market with the goal of complementing existing product offerings, capturing market share in what was expected to be a rapid growth segment, and, naturally, producing an underwriting profit. Initially, most of the cyber insurers achieved these goals. Over the past 15 years, additional insurers, MGAs and insuretechs entered the cyber marketplace. This influx of capacity ultimately led to broad coverage and low premiums – truly a buyers' (or soft) market.

In addition to broad coverage and low premiums, many carriers simplified and streamlined the application process. The original comprehensive applications were narrowed down to just a handful of underwriting questions. Recently, some carriers have developed an underwriting process that only requires the submission of the prospective insured's website. Notwithstanding these concessions, taken as a whole, the cyber marketplace still produced an underwriting profit.

The evolution of the cyber product over the past decade has resulted in the following: (1) Low premiums as a result of competition among both legacy cyber insurers and new entrants to the marketplace; (2) Broad coverage which has resulted in policies being more responsive to both historical cyber exposures and newly emerging cyber risks; (3) Mature cyber claims data which has yielded better insight into which risk factors are driving cyber losses; and (4) The overall insurance industry starting to place cyber exclusions on their non-cyber policies, such as Property and General Liability, to clarify that those policies will not respond to cyber claims. This removal of so-called "silent cyber" has pushed more non-buyers to purchase stand-alone cyber policies and has generally elevated the profile of cyber coverage.

The Evolution of Cyber Exposures

As cyber coverage and exposures have evolved, we have seen the introduction of a constant cadence of new cyber-related acronyms such as PCI, PII, PHI and BEC, as well as terms such as "social engineering," "bricking," and "phishing attacks." At the same time, the cyber regulatory environment has continued to expand and intensify. The General Data Protection Regulation, the Illinois Biometric Information Privacy Act and the California Consumer Privacy Act, to just name a few regulations, have brought heightened attention to cyber exposures, risk mitigation, and regulatory compliance. While all of these issues are important, no acronym, term or regulation has caused more consternation for cyber insurers than the rapidly increasing frequency of, and losses caused by, ransomware attacks. Underwriters are grappling with both the amount and severity of ransomware attacks which have had a material negative impact on the profitability of cyber insurance over the past two years. Ransomware attackers have also realized that they can demand and receive much higher ransom payments than in the past. According to cybersecurity firm Coveware, the average ransomware payout has grown from less than $10,000 per event in 2018 to more than $154,108 per event in the 4th quarter of 2020. Insurers are citing some ransomware demands to be in the seven figure range. In many cases, the attackers also steal data from their victim organizations which exposes the target to a data breach on top of the ransom demand, further compounding cyber insurers' exposures. As if all of this wasn't enough, the proliferation of remote work arrangements might expose companies to a range of new vulnerabilities to cyber attacks.

There is a misconception that cyber risk is mainly limited to large companies. According to the most recent NetDiligence Cyber Claims Study, incident costs continue to increase, and the majority of

CONTACT
RT Specialty
D: 312-784-6001
RTProExecInfo@rtspecialty.com
180 North Stetson Avenue
Suite 4600
Chicago, IL 60601

RT ProExec

cyber incidents (98%) have shifted to Small to Medium Enterprises (SMEs) as opposed to larger companies (organizations with $2 billion or more of annual revenue). While the overall costs of breaches at larger companies are naturally higher, the risks to SME's is higher than it has ever been.

Current Market Conditions

As a result of the foregoing, the cyber insurance market is firming. Many insurers are increasing both premiums and retentions, and many underwriters are asking additional underwriting questions, with an emphasis on internal controls for preventing ransomware and establishing risk management controls. At least one leading cyber insurer has materially restricted coverage for insureds with inadequate internal controls by capping all ransomware related losses to the lower of 50% of the aggregate limit or $5 million. Additionally, this insurer is applying a 50% coinsurance to all loss over the retention. Further, in response to the SolarWinds data breach and the potential resultant breaches at a wide swath of U.S. government agencies and technology companies, another leading cyber insurer has introduced an exclusion on its renewals and new business quotes for claims related to the SolarWinds breach. While the restrictiveness of this exclusion is troubling in its own right, it also provides some insight into how insurers may react as other systemic events occur in the future. At minimum, it highlights how a breach at one company can have much larger impacts across the economy and the cyber marketplace.

It remains to be seen whether the balance of the cyber marketplace will limit coverage as described above or in other new ways. However, we do expect insurers to continue to examine the profitability of their respective books of business, with an emphasis on raising premiums and retentions and being very diligent in their underwriting, with particular emphasis on internal cyber loss controls. It is possible that, in the future, broad terms and conditions may only be available to insureds with strong internal controls.

Renewal Expectations

As renewals approach, all things being equal, we expect to see the following from the marketplace:

- Questionnaires that focus on insureds' cyber risk management controls. The answers to the questions may impact how the insurer will cover ransomware risk as well as the overall coverage, premium and retention levels;
- For mature insurers, SME businesses should be prepared for at least 10% - 30% increases in premium (above and beyond rate changes due to revenue growth). Some newer underwriting facilities are beginning to increase premiums as well, but in the 10% - 15% range. For insureds who have had cyber claims or who have inadequate internal controls, premiums may increase by 50% or more;
- For larger businesses (those with revenue greater than $1 billion), we expect premium increases in the 10 - 20% range;
- Insurers may reduce limits for certain renewals. This may result in a need for new relationships with excess insurers to seek additional coverage;
- Given the increasing severity of losses, excess insurers may seek higher increased limit factors than they have in the past, which means their rate increases will be larger on a percentage basis than the primary layer;
- As underwriting facilities re-underwrite their respective books of business, it is possible that they will non-renew insureds in certain industries or with financial sizes outside of their revised appetites. We will continue to monitor insurers changing risk appetite.

We are always hesitant to provide premium guidance as things change so quickly in the insurance marketplace. However, as of the date of this article, we feel that these ranges are a reasonable prediction. The cyber market will remain fluid and highly dependent on underwriting results.

We highly recommend starting the renewal process as early as possible to avoid surprises. The timely completion of applications, questionnaires – and properly addressing potential follow-on questions will help secure favorable results – albeit at a potentially higher premium. Given that the cyber market is in a state of constant change, we will continue to provide updates as things develop.

CONTACT

RT Specialty
D: 312-784-6001
RTProExecInfo@rtspecialty.com
180 North Stetson Avenue
Suite 4600
Chicago, IL 60601

RT ProExec