RT ProExec
INSIGHTS
VOLUME XXIII ISSUE 2 SUMMER 2021

CYBER INSURANCE: DETERIORATING UNDERWRITING RESULTS AND ITS RAMIFICATIONS

As of the publication of this InSights newsletter, another major breach has made the headlines. T-Mobile announced that a cyberattack accessed personal information linked to about 7.8 million current subscribers and records of about 40 million people who previously applied for credit with T-Mobile. It is too early to estimate the cost of the breach, but T-Mobile stated that it will offer two years of free identity protection from McAfee, along with other services, to its customers. We fully expect regulatory scrutiny will ensue. This breach is but the latest example in an onslaught of cyberattacks that is increasing in both frequency and severity and, as a result, is roiling the market for cyber insurance.

Cyber insurance underwriting results have deteriorated at an alarming pace. According to an AM Best cyber insurance report dated June 2021, the 2020 combined ratios for the top 5 insurers averaged 104.1%, while the top 10 insurers combined ratio averaged 100.7% and the top 20 averaged 96%. AM Best further reported that 3 of the top 5 insurers had estimated combined ratios of 123%, 125.8% and 117.2% for 2020. For non-insurance savvy readers of this article, the combined ratio is a measure of insurer profitability. Generally speaking, and before factoring investment gains or losses, a combined ratio under 100 indicates an insurer is making an underwriting profit and a ratio over 100 indicates an underwriting loss.

Coalition, a leading provider of cyber insurance and security, recently released their Cyber Insurance Claims Report for the first half of 2021. The report is comprised of data on Coalition's policyholders, which includes a wide range of insureds with up to $1 billion in annual revenues. The report highlights some key comparisons of the first half of 2021 to the first half of 2020.

- Business email compromise (BEC) incidents were the most frequently reported claims. BEC incidents are up 51%
- The average ransomware demand in the first half of 2021 was $1.2 million, an increase of nearly 170% over the prior period
- The frequency of incidents reported by organizations with under 250 employees increased 57%

Additionally, during the first half of the year, concerns over the cyber vulnerability of the U.S. infrastructure took front stage. A ransomware attack against Colonial Pipeline turned off the spigot on the largest pipeline system for refined oil products in the U.S. The attack prompted the company to shut down for nearly a week. This led to long lines at gas stations, panic-buying, fuel shortages and elevated fuel price spikes. In the past, it could be argued that cyber security was a rather abstract issue for the general population, but the Colonial Pipeline situation made the threat seem very real, very quickly.

While this attack might have turned cyber into a current hit, it is just one of the latest notes in a song that has been getting much more air play with cyber insurers over the past 18 months.

The insurers participating on the Colonial Pipeline cyber insurance program will likely reimburse the company for the $4.4 million paid in response to the ransomware demand. Unfortunately, this is not the extent of the potential exposure, as the cyber insurers likely know all too well. Other coverages, such as business interruption, restoration, forensic work and other therapeutic measures, could increase the insured loss. In a very interesting twist, as of the date of this publication, the FBI disclosed that it seized $2.3 million of bitcoin allegedly held by Darkside, the hacking group that targeted

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

RT ProExec

Colonial Pipeline. We will continue to monitor this development and its ramifications for the cyber marketplace.

On the heels of the Colonial Pipeline breach, JBS S.A. (JBS) was hacked. JBS is the largest (by sales) meat processing company in the world. The cyberattack halted operations and further slowed the food-supply chain, which was already under significant stress from labor shortages, production constraints and high transportation costs. JBS confirmed that the company paid $11 million in ransom to the hackers. As of the date of this publication, we are not aware of the cyber insurance program in place and whether insurance has reimbursed for the ransom payment. What we do know, is that JBS has stated that it spends more than $120 million annually on IT and employs more than 850 IT professionals globally.

The attacks on U.S. infrastructure have led the Biden administration to more aggressively police companies' security standards and privacy safeguards. While many governmental agency officials provide recommendations on best practices, shortly after the Colonial Pipeline hack, the Transportation Security Administration (TSA) rolled out regulations, including a requirement that pipeline operators report cyberattacks. This may be a harbinger for more regulations to follow.

The infrastructure industry would not seem to be the only vulnerable segment. All entities, across all industries, likely have some degree of susceptibility to a cyberattack. For instance, the Financial Stability Board (FSB), an international body that monitors and makes recommendations about the global financial system, stated that cyber activities, inclusive of phishing, malware and ransomware, grew from less than 5,000 per week in February 2020 to more than 200,000 per week in late April 2021. The FSB stated that the surge of cyberattacks on the financial services sector will continue as staff continue to work from home.

Partially as a result of the points discussed above, we are seeing that primary cyber insurers are generally pulling some or all of their levers to return to underwriting profitability, such as substantially increasing premiums, reducing limit capacity (especially when the limit is greater than $5 million), increasing retentions, and restricting coverage. On excess placements, underwriters are following the primary and underlying percentage increases in premiums, and at times, increasing premiums at a higher percentage basis — as well as reducing capacity and coverage. To this end, during a recent analyst conference call, AIG CEO Peter Zaffino said, "We continue to carefully reduce cyber limits and are obtaining tighter terms and conditions to address increasing cyber loss trends, the rising threat associated with ransomware and the systemic nature of cyber risk generally."

Cyber insurance has quickly become a high frequency / high severity coverage line. This is, in our experience, an unforgiving combination for insurers. Historically, cyber had been a profitable line for most insurers in the space. Suddenly, carriers are experiencing declining profit margins and, in the worst cases, underwriting losses. The cyber markets as a whole are generally weighing factors such as the potential for catastrophic cyber losses, the short-tail and long-tail nature of cyber risks, the supplier / vendor vulnerabilities that can lead to systemic losses that affect multiple policyholders and a heightened and evolving regulatory environment.

Cyber underwriters generally are paying much closer attention to insureds' risk management policies and practices. As such, in our experience, nearly all insurers now request supplemental underwriting questionnaires or ask additional questions about loss control policies. The answers to the questions will positively or negatively impact the markets' terms and conditions. Unsatisfactory answers will likely lead to declinations and even non-renewals.

In light of the upset in the market, we thought it would be beneficial to ask a few questions to one of the leading global participants in the cyber market. We are pleased that Bob Wice, Head of Underwriting Management, Cyber & Tech, from Beazley Group has generously agreed to spend some time speaking with us.

RT ProExec: As one of the largest cyber markets, please provide your assessment of the cyber insurance market.

Mr. Wice: The cyber insurance market tends to evolve quickly, and 2021 has been no exception. As the ransomware threat has increased, underwriting appetites have varied depending on size of insured

CONTACT

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

RT ProExec

and claims experience across different industries. Assessments of frequency and severity can change month to month, and due to the short tail nature of cyber claims, markets have reacted quickly with focused risk selection, increased rate goals and management of limits and retentions. While capacity for lower limits in the SME space persists, larger organizations have fewer primary options, and brokers have found it increasingly difficult to build excess limits.

RT ProExec: Given the high frequency and severity of claims, how do you underwrite towards sustainability?

Mr. Wice: Data analysis is the key. We are working with brokers to collect details on critical risk management controls in a structured way to determine which of those controls can make a difference in preventing frequency and mitigating severity. External vulnerability scans are also playing a role in identifying risk factors which can lead to the increased probability of a loss.

RT ProExec: As an industry, we often fail to discuss the basics. What are the risk management safeguards that companies must adopt to secure quotations with favorable terms and conditions?

Mr. Wice: A defense in depth and layered security approach to cyber risk management will help avoid significant losses. When email security tools fail to prevent initial systems compromise due to human error, internal security controls such as multi-factor authentication for privileged user accounts, network segmentation and proper logging and monitoring will help prevent the spread of an attack. Failing that, segmented backups and frequent testing of restoration capability are keys to demonstrating favorable cyber risk management controls.

RT ProExec: The insurance industry is under considerable criticism for insuring ransom payments. Elected officials and government branches, including the FBI, discourage the payment of ransom payments — often citing that it enriches and emboldens criminals and essentially funds more attacks. Recently, at the insistence of the French government, a major global insurer stopped insuring ransom demands under cyber insurance policies in France. As France only trails behind the United States in the payment of ransom demands, do you see the recent action as a barometer for changes in coverage in the United States?

Mr. Wice: The increased attention to extortion payments at the government level is a positive development. It is a question for governments to decide on public policy with respect to ransomware payments. We are not excluding extortion payments from our policies, but we will comply with local regulations, if enacted. We intend to continue to focus on helping insureds establish more robust risk management practices to strengthen their defenses against these evolving threats.

CLOSING THOUGHTS

As the cyber insurance market continues to evolve, we will closely monitor the many moving parts discussed above. Irrespective of the market dynamics, in the unfortunate event of a cyber incident, we remain your steadfast advocate. Our advocacy commences by fully recognizing that organizations experiencing a cyber incident are victims. It continues by recognizing that those who perpetrate these hacks are criminals. From the outset, it is paramount for us, the market(s) and the policyholder to be singularly aligned to meet the challenges of a cyber incident. We understand the sensitivity and criticality of a cyber breach as well as the importance of enhancing communication, explaining the process and working together to achieve a favorable outcome.

CONTACT

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

RT ProExec

RT ProExec is a part of the RT Specialty division of RSG Specialty, LLC, a Delaware limited liability company based in Illinois. RSG Specialty, LLC, is a subsidiary of Ryan Specialty Group, LLC (RSG). RT ProExec provides wholesale insurance brokerage and other services to agents and brokers. RT ProExec does not solicit insurance from the public. Some products may only be available in certain states, and some products may only be available from surplus lines insurers. In California: RSG Specialty Insurance Services, LLC (License #0G97516).
©2021 Ryan Specialty Group, LLC