2022 Q2

State of the Cyber Market

By Steve Robinson, RPS National Cyber Practice Leader

As we are finally able to jump off the treadmill that was pegged on level 10 in the run-up to July 1, 2022, now is a good time to pause, take a breath and look back at the virtual ground we covered. It's also a good time to look ahead to what is in front of us, as 2022 is shaping up to be a pivotal year in the chronology of cyber insurance development.

With each quarterly cyber insurance update, we look at the market from several angles. In keeping with that approach, we'll assess the current environment, checking in on areas such as cyber insurance coverage, pricing, carrier appetites, underwriting trends and the regulatory landscape. We'll also check in on loss trends in RPS' own book of business, gleaning insight from the tens of thousands of U.S. policyholders whose agents place their cyber insurance coverage through RPS.

CYBER COVERAGE AND CARRIER LANDSCAPE

We continue to see an increase in the number of carriers employing sublimits in various capacities in an effort to reduce the financial impact of ransomware events on the industry. Agents should pay close attention to exactly how these sublimits are used, as carriers are taking various approaches to limiting their exposure.

For instance, some will sublimit coverage for ransom payments only, while others are applying a sublimit to the entire policy if the cause of loss was a cyber extortion (ransomware) event. These details are very important to point out when advising your clients on their next renewal because not all insurers are making these changes very clear.

Oftentimes, a quick read of the declaration page won't be sufficient; you will have to dig deeper into the endorsements to understand the full impact. When they experience a claim, this extra effort could determine whether your client's coverage is coming from their cyber insurance policy or your E&O.

Speaking of endorsements, one thing is clear: As cyber insurance has moved from the land grab that was 2015 to 2020 to the maturing stages we are currently in, carriers are more mindful than ever of their potential exposure to systemic risk.

Among the major concerns is the prospect of a breach of a major cloud services provider (CSP). After giving credit to the information security posture of CSPs, one industry expert noted, "On the other hand, I'd never bet against the bad guys in the long run. There are just so many of them, a lot more than you ever know of. So, would I bet a paycheck that we'd go a whole year without such a major breach happening? No."[1]

Among the major concerns is the prospect of a breach of a major cloud services provider.

Much like war and terrorism to property insurance policies, systemic risk has traditionally not been priced into the sustainability of cyber insurance. How could it? As a result, we are beginning to see more endorsements designed to limit coverage for zero-day attacks, widespread events, common CVE vulnerabilities and neglected software. Be sure to look at expanded definitions of infrastructure that amend existing exclusions in the policy beyond the traditional satellite/electrical/mechanical variety to now include internet service providers and even cloud providers.

Again, these endorsements can have a significant impact on coverage, so be sure to understand how the policies are changing. What's more, at times, these new endorsements can have innocuous titles that don't accurately reflect the fact that coverage has just been reduced significantly.

The dialogue continues regarding insurers' varying approaches to addressing war and terrorism. The war in Ukraine has cast a light on this as the combination of armed conflict and digital warfare comes more into focus. As a result, we are seeing new exclusions specifying the fact that insurers have no intention of covering acts sponsored by nation-states or in conjunction with a traditional physical war of any kind.

WHERE PREMIUMS STAND

We have found ourselves in a period of necessary retraction, as insurers pull the various levers of rate, sublimits, coverage restrictions and underwriting scrutiny to ensure profitability. And as cyber insurance demand and rates have both continued to climb, many insurers are seeking more balance to their portfolio, having found themselves cyber-heavy. As a result, competition is heating up in professional liability, D&O, EPLI, crime—really all areas of executive liability outside of cyber.

Premium increases are still there, but flattening, and an underwriters' tool of choice is more often scalpel than machete when making decisions on their cyber book of business. Capacity continues to be a concern for many as we enter the second half of 2022.

That said, we feel the future is bright for cyber insurance as loss development further informs the right combination of underwriting standards, coverage terms, limits deployment and rate.

July 1 renewals brought significant premium increases, although not as high as those realized in July 2021 in many cases. Interestingly, the predictability of 2021 has given way to myriad approaches that can, at times, have little rhyme or reason. The more loss-sensitive classes of manufacturing, public entity, education and construction are either on the do-not-write list for many or often require deep-dive underwriting in order to get terms. Once terms are secured, we are seeing vast differences as well.

Case in point: In the 2021–2022 policy period, we had a manufacturing client ($30 million in annual revenues) obtain a $5 million limit x $10,000 retention at a premium of $15,000—yes, the deal of the century as we look through the lens of today. Fast-forward to this most recent renewal cycle—after an exhaustive look under the hood at relationships between information and operational technologies in their production process, the insured was non-renewed by their incumbent carrier, despite having no claims. Marketing efforts yielded results that generated premiums ranging from $30,000 to $92,000 with retentions ranging from $25,000 to $100,000. This demonstrates the volatility of the market right now, particularly in an industry class that many reports have cited as the most attacked in 2021.[2]

Conversely, tower excess placements in difficult classes like public entity achieved improved results in isolated instances this cycle. As an example, a large western county that was only able to obtain $10 million in first-party limits last year was able to round out their tower with $30 million in limits for both third- and first-party coverage, effective July 1, 2022. The coverage was costly, but changes, particularly in the U.S. domestic market, yielded additional capacity at the right price that wasn't previously available. Additionally, like many insureds, the county made significant investments in MFA, managed endpoint detection and response, and segmented backup solutions, all of which helped them earn favor with insurers.

A PERSONNEL DROUGHT AND THE WAR FOR TALENT

Many accounts that were previously no-touch are requiring more time, effort and know-how to get the best result for insureds. With more work comes the need for additional staff, and this points to a growing concern in the cyber insurance marketplace: personnel.

There is a war for talent as we have witnessed unprecedented career movement among the insurer and brokerage community. This disruption has led to costly delays and increased frustrations as we approached the 7/1 renewal cycle. Fortunately, RPS has not experienced this turnover nearly to the extent of others, leading us to take a different approach with an "I'm Staying…" campaign on LinkedIn that featured employees with no intention of switching firms. The campaign garnered a lot of positive response and some laughs as we shined a light on the employment trends around us.

LEARN THE LANGUAGE

Today's insurance agents must become more familiar with highly technical elements in the cyber underwriting process. If they aren't, they need to partner with someone who is. As the applications are increasingly loaded with tech jargon, it is important that insureds engage their IT staff or outsourced vendors to ensure that the representations in the policy are accurate. And it is equally important that agents understand what the applications are asking and communicate the potential consequences of getting it wrong, should a claim occur.

Earlier this month, in a court filing in Illinois, one insurer asked for a ruling to rescind a policy due to the insured's alleged misrepresentation that it had multifactor authentication (MFA) in areas where it did not.[3] The insured, an electronics manufacturing services company, suffered a ransomware attack, and the investigation revealed inconsistencies between what they represented in their application and what was actually in place on their network. As MFA was the most used and least understood acronym of 2021 in our industry, we suspect this won't be the last of such disagreements between insurers and their insureds in the months to come.

THREAT LANDSCAPE

From a threat perspective, we continued to see reductions in frequency and severity of ransomware losses in Q2, right up through the end of June. July is showing an uptick that we will be watching to see if the first half of 2022 was an anomaly.

One research firm points to the significant share of ransomware activity attributed to Russia-linked hacking groups.[4] Many speculate that the war in Ukraine has been responsible for the slowdown, as significant players in the region have been more inwardly focused.

We would like to think that a combination of improved infosec controls among small and midsize businesses (driven, in large part, by more in-depth underwriting requirements to obtain cyber insurance[5]), coupled with increased media and government focus on ransomware attacks, has helped stem the tide. Regardless of the causes, these are welcomed trends for insurers and their customers alike. As long as ransomware is a) lucrative and b) anonymous, we believe the frequency and severity trends may ebb and flow over time, but they won't go away.

Hive[6] and Vice Society[7] are examples of ransomware variants affecting small- to medium-enterprise (SME) clients in June. Double and triple extortion have become more and more woven into the fabric of these ransomware claims, as threats of data exfiltration and distributed denial of service attacks (DDoS) are leveraged as additional means to get victims to pay.

Among RPS' tens of thousands of SME cyber insurance policyholders, the month of June's most prevalent claims were fraudulent payments (45%), followed by ransomware (20%) and social engineering (15%). For clarity's sake, fraudulent payment is an incident where the insured was duped into sending funds (usually through some sort of social engineering scam). Social engineering means phishing scams that did not result in a loss of funds (it may have been a failed attempt or a non-monetary attack, like credential harvesting, etc.). We separate these so as not to double-count loss matter types. We have also witnessed an increase in the number of third-party lawsuits relative to data/privacy.

From an affected industries perspective, the manufacturing sector led the way with 20% of reported matters among our SME policyholders, followed by construction (15%), professional services (10%), education/schools (10%) and charities/not for profit (10%).

REGULATORY ENVIRONMENT

The American Data Privacy and Protection Act (ADPPA) is a bipartisan bill in the House of Representatives designed to give U.S. citizens greater rights over their personal data. The bill "aims to restrict the uses and disclosures of the personal data of citizens without consent, will give consumers a host of new rights over their personal data, and there is also a private right of action, which will allow consumers to take legal action against entities that violate their privacy and misuse their personal data."[8]

Hearings took place on June 23, and there are still potential stumbling blocks relative to preemption of current state privacy laws and the private right of action, leaving some concerned about a potential wave of lawsuits if the bill is ultimately signed into law. We will be monitoring the progress of this legislation and the impact it may have on the cyber insurance marketplace.

LOOKING AHEAD

There are some key questions that will shape the next quarter, and arguably the very future of cyber insurance. Will the downward trend in ransomware losses continue? Will the upward trajectory of premiums continue to flatten? Will the infusion of technological capabilities in the underwriting process yield improved loss ratios? Will the wave of exclusions relative to systemic risk, critical vulnerabilities, cyber attacks accompanied by armed conflict and unpatched software become the norm among cyber insurers? Will they have their desired effect, and will this dilution impact buyer behavior? Will there be a major CSP breach that turns the market on its head?

While we don't have all the answers, we are bullish on the future as we see signs of progress in a product that is continually maturing.

We have noted before—unlike age-old perils of wind, water and fire, the very essence of cyber risk is continually changing, adapting in real-time to its environment in ways Mother Nature has never shown us. Such a dynamic risk requires the best minds in the business and creates enormous opportunity for the next generation of insurance professionals. Among the constant pace of change, having a trusted partner with broad access to the marketplace and deep knowledge of the changing coverage landscape is more important than ever. RPS is happy to be leading the way in this constantly evolving process, and we look forward to the innovation and opportunity that lies ahead.

[1] "Splunk Data Security Predictions 2022," Splunk.com.
[2] "X-Force Threat Intelligence Index 2022," IBM Security. February 2022.
[3] "Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use," Chad Hemenway, Insurance Journal, July 12, 2022.
[4] "74% of Ransomware Revenue Goes to Russia-Linked Hackers," Joe Tidy, BBC.com, February 14, 2022.
[5] "Cyber Insurers Are Starting to Require Lateral Movement Defense. Here's Why," John Anthony Smith, SecurityMagazine.com, June 23, 2022.
[6] "HC3: Analyst Note—Report 202204181300," HHS Cybersecurity Program—Office of Information Security, April 18, 2022.
[7] "Latest Vice Society News," Bill Toulas, Bleeping Computer, June 27, 2022.
[8] "American Data Privacy and Protection Act (ADPPA) Formally Introduced," Compliance Junction, July 4, 2022.