# 2022 Q1: State of the Cyber Market

Steve Robinson
RPS National Cyber Practice Leader

On the heels of the most rapidly changing year for cyber insurance coverage to date, the first quarter of 2022 showed no signs of yielding that distinction to its predecessor. Agents, brokers and insurers continue to navigate constant change in capacity, terms and conditions, and the threat landscape in an effort to keep cyber insurance a critical element of their insureds' risk management programs.

With an insurance coverage as dynamic as cyber, it is helpful to look at updates through several lenses: claims trends, market movement, regulatory landscape, geopolitical influence and coverage dynamics.

## CLAIMS TRENDS

As discussed in our 2021 RPS Cyber Market Outlook, ransomware led the way last year in cyber insurance claims frequency and severity for most insurers. Further, one information security firm recently noted that the exfiltration of data associated with ransomware attacks increased by more than 82% in 2021. The threat of data release and distributed denial of service (DDoS) attacks has added complexity and expense to ransomware claims, and insurers took notice. Industry experts further note that ransomware tactics continue to evolve beyond restricting access to data in exchange for payment. In 2021, threat actors claimed to have stolen data 82% of the time compared to 70% of the time in 2020.

As we entered the opening days of 2022, it appeared that the New Year would not only rival, but perhaps surpass, the headlines generated in the previous 12 months. In January, we witnessed significant ransomware attacks on a community college and a large western county affecting operations well beyond mere computer networks. These attacks disrupted the functionality of HVAC systems, lighting and security systems, including locking mechanisms and video surveillance in a corrections institution. As organizations continue to increase their reliance on internet connectivity for every part of their operations, these attacks impose crippling disruption to operations, finances and even physical safety.

Interestingly, however, in stark contrast to the early signs that January showed us from midsized to larger organizations, RPS's small business sector of clients have reported a 35% reduction in the frequency of ransomware related events in Q1 2022. Some theorize that the increased attention to the ransomware pandemic given by the Biden administration, and a heightened news focus, have led to at least a temporary slow-down in activity of this nature.

Additionally, as ransomware events continue to garner headlines, organizations have made more deliberate efforts to steel themselves from their effects. Lastly, we believe the insurance community has played a pivotal role in moving the needle for organizations to take their information security defenses more seriously. If they want cyber insurance coverage, they have to comply with minimum standards–which, by the way, are far more in-depth than those previously required.

Social engineering and wire fraud losses have moved to the forefront of claims frequency in Q1. In the month of March, social engineering/fraudulent payments accounted for 54% of total reported incidents in our

SME segment. More so than ransomware, these types of claims are often highly preventable with the most basic, nontechnical checks and balances in place. Insurers have moved back into pre-2017 mode, most requiring that call-back procedures are in place before agreeing to offer limits for social engineering/cyber deception. As the workforce transitions between work-from-home to in-office configurations, cybercriminals are taking advantage of the disruption in normal operating procedures, capitalizing on this hybrid/agile work environment to carry out their crimes.

Cybersecurity and incident response firm Tracepoint adds, "Business email compromise activity has remained consistent, especially as the deadline for personal tax filings in the U.S. draws closer and given that a number of organizations are filing for extensions on the corporate tax deadline which passed on March 15th."

## MARKET MOVEMENT

The loss ratios of 2021 have continued to put pressure on available capacity for cyber insurers, both domestically and abroad. The close of the quarter brought news of a once-prominent MGA's withdrawal from the cyber market after unsuccessful attempts to renew approximately 80% of its binder. Capacity restrictions have been felt in additional ways, including a temporary pause in new business writings from some markets and the elimination of $5 million limits by others, in addition to significant de-risking in more loss-sensitive sectors of business such as public entity, education and manufacturing.

At the same time, we continue to note significant increases in rate, ranging from 30% to 200% or higher, depending on industry, risk posture and prior loss experience. The steep upward trend in premiums really started to take hold in the surplus lines market around mid-2021. For admitted coverage, the increases rolled out more incrementally throughout the U.S. as state filings were reviewed and subsequently approved. This process continues into 2022. As a result, many insureds have yet to experience the first wave of sticker shock that is coming their way, while others are preparing for round two.

Further underscoring the unpredictability of the current cyber insurance market, as we track increasing rates on the vast majority of our book, we have simultaneously witnessed for the first time in three years flat rates for certain insureds. As the sophistication and accuracy of outward-facing network scanning technologies continues to improve, some insurers are rewarding those risks showing best-in-class controls with flat, sometimes even slightly lower, premiums. This is an encouraging sign, although we have thus far only seen these results in isolated circumstances and don't expect this to become a trend any time soon. For larger organizations, carriers are increasingly involving outside cybersecurity consultancy firms to bolster their expertise as they identify best-in-class risks and move away from those believed to present the greatest risk.

While we don't believe that rate increases north of 100% present a sustainable model if pushed through multiple renewal cycles, we do not anticipate a softening market in 2022. Insurers understand that increasing rates alone will not ensure the cyber insurance market's sustainability. Finding the right combination of rate, underwriting discipline, retention and limits management will be required.

We have also witnessed a move by many carriers to shortened timelines for quote. The once-common 60-day window has been taken to 30 days out from renewal for many markets for two reasons: 1) staffing adequacy is a real problem in the industry as demand has outpaced many carriers' ability to keep up; and 2) the constantly evolving pace of new threats means carriers want as much time as possible to account for the next discovered systemic vulnerability. Shorter windows afford them more time to incorporate relevant exclusions in their wordings, whenever they feel it is appropriate.

## REGULATORY LANDSCAPE

In November of 2021, North Carolina became the first state to declare it illegal for state agencies and local government entities (including public school districts) to pay a ransom following a ransomware attack. The budget appropriations bill also outlined reporting provisions for cybersecurity incidents to the Department of Information Technology.

There is debate in some circles as to whether or not actions such as this will help or hurt in the fight against these pervasive threats. Bryan A. Vorndran, assistant director of the FBI's Cyber Division said in remarks before a U.S. House Judiciary Committee hearing that banning ransom payments could potentially create what is known as a "triple extortion" situation. Vorndran argued that cybercriminals can already encrypt a company's network and demand payment, but also steal data from companies to use for additional blackmail if the attack is reported.

He testified, "It would be our opinion that if we ban ransom payments, now you are putting U.S. companies in a position to face yet another extortion, which is being blackmailed for paying the ransom and not sharing that with authorities."

These were notable remarks, particularly because the FBI's position has traditionally been to advise organizations to not pay a ransom. It isn't clear whether these remarks signal a change in posture (doubtful), or, simply recognition that there are instances where, as a business decision, there is no other choice.

In the first quarter, we have seen additional legislative activity on the federal side as well. On March 15, 2022, President Biden signed the 2022 Consolidated Appropriations Act into law. Within the legislation is the Cyber Incident Reporting for Critical Infrastructure Act of 2022. This act establishes new cybersecurity reporting requirements to the Cybersecurity and Infrastructure Security Agency (CISA) no later than 72 hours after a cyber-incident and within 24 hours after a ransom payment has been made.

It was noted that these provisions, by affecting 16 defined critical infrastructure industries, will likely "apply to businesses in almost every major sector of the economy, including healthcare, financial services, energy, transportation and commercial facilities." Information sharing between the private and public sector will continue to be critical in the fight against cybercrime of all varieties.

## GEOPOLITICAL INFLUENCE

The crisis in Russia and Ukraine is already impacting underwriting in the cyber insurance community. Insurers are concerned that sanctions imposed on Russia will lead to an increase in cyber attacks emanating from the region. The ransomware analytics and response firm Coveware recently stated that this new environment "could lead to an explosion in the volume of people that turn to ransomware as a means to support themselves. The isolation that Russia now faces has the potential to create a perfect safe haven for cybercriminals".[i]

A Moscow-based cybersecurity firm with more than 400 million users worldwide was recently added to the FCC's list of restricted entities. Brendan Carr, FCC commissioner, commented that the ban will "help secure our networks from threats posed by Chinese and Russian state-backed entities seeking to engage in espionage and otherwise harm America's interests."[ii] And with this action, we are already seeing some insurers craft exclusions relative to potential exploits, causing insureds to scramble for replacement of their endpoint detection and response solutions.

Given the situation in Ukraine, discussions around war exclusions in cyber policies have taken on renewed importance. Most cyber insurance policies specifically exclude war but offer carve-backs for acts perpetrated electronically. Still, details such as the ability to determine attribution and the definition of "war" are among the topics that contribute to a sense of ambiguity, and insurers are seeking to provide additional clarity in their wordings.[iii] We continue to monitor changes in this area.

## COVERAGE DYNAMICS

As cyber threats continue to evolve, so too do underwriting techniques and the coverage grants found in cyber insurance policies. If 2018 brought about a furious stretch of cyber insurance product innovation, 2022 is ushering in a retraction in terms and conditions at a similar pace.

The first quarter has seen wider adaptation of restrictive policy language by some insurers in areas such as Common Vulnerabilities and Exposures (CVE) identified by the National Institute of Standards and Technology (NIST), systemic risk or aggregate risk, end of life (unsupported) software and a continued pullback in available limits–often times across all insuring agreements–for any loss stemming from a ransomware attack.

Ransomware claims typically trigger multiple insuring agreements in a cyber insurance policy beyond extortion, including business interruption, data restoration, forensics, legal, and notification expenses when the claim also involves unauthorized access to personally identifiable information. For this reason, insurers are often moving beyond just the ransom payment itself when sublimiting coverage. It is important to look closely at the fine print as these terms and conditions continue to change.

We are also witnessing both vendor and event-specific exclusions and additional underwriting scrutiny tied to specific software platforms connected with widely-reported exploits, and, as previously mentioned, vendors who are associated with nation states that are alleged to be less than U.S.-friendly. Some carriers have designed exclusionary wording broad enough to contemplate future events such as these in a "Insert New Vulnerability here _____" type of fashion. This is concerning as the level of technical understanding in the insurance community needs to increase if organizations are to be properly informed of the cause-and-effect impact of policy revisions such as these.

## THE ROAD AHEAD – THE FIVE PS

Changes in the process, players, products, pricing and political landscape associated with the cyber insurance market will continue to challenge agents, brokers and insurers in the months to come. As we prepare for the onslaught of July 1 renewals, the greatest difficulties will be felt in the education and public sectors, as the number of insurers willing to entertain these sectors has dramatically constricted, both in the primary and excess markets. The needle is always moving, and, regrettably, many education and government agency risks will find themselves without a viable cyber insurance option. We see the insurance community playing a pivotal role in driving the improvement of information security defenses among both public and private sector organizations.

The heightened E&O exposure for insurance agents who are not well-informed of the frenetic pace of change in this market is extensive. Now, more than ever, it is important to partner with a trusted broker with extensive expertise in navigating these changes. While this market is certainly challenging, it also presents opportunities for more in-depth discussions and the best agents will be able to leverage this to show increased value as trusted advisors. With a large team of cyber insurance experts across the entire U.S., exclusive products and broad market representation, RPS stands ready to assist our retail agency partners to ensure the best outcome for our mutual clients.

**Sources**


[1] "2022 Data Security Incident Response Report", Baker Hostetler, Theodore J. Kobus III et al, April, 2022

[1] "Biden Administration Takes new Steps to Combat Ransomware Attacks", Edward Segal, Forbes, September 21, 2021

[1] "How the Russian/Ukraine War May Lead to an Explosion in Ransomware Attacks", Coveware Blog, March 25, 2022

[1] "Kaspersky Blacklisted by FCC alongside China Telecom and China Mobile", Campbell Kwann, ZDNet, March 27, 2022

[1] "Munich Re Tightens Up Cyber Insurance Policies to Exclude War", International Business Times, Carolyn Cohn and Noor Zainab Hussain, April 8, 2022

[1] "NC Prohibits Agencies from Paying Ransoms" Susan Miller, GCN, April 8, 2022

[1] "Optio MGA Ascent Withdraws from Cyber Market in Failed Binder Renewal" Catrin Shi, Insurance Insider, March 31, 2022

[1] "President Biden Signs into Law the Cyber Incident Reporting Act, Imposing Ransomware Requirements for Cyber Incidents and Ransomware Payments" National Review, Volume XII, Number 101

[1] "The CrowdStrike 2022 Global Threat Report"

[1] "Top FBI Official Advises Congress Against Banning Ransomware Payments", Maggie Miller, The Hill, July 27, 2021

[1] "Tracepoint Weekly Update", Brendan Rooney, April 5, 2022


---


[i] "How the Russian/Ukraine War May Lead to an Explosion in Ransomware Attacks", Coveware Blog, March 25, 2022

[ii] "Kaspersky Blacklisted by FCC alongside China Telecom and China Mobile", Campbell Kwann, ZDNet, March 27, 2022

[iii] "Munich Re Tightens Up Cyber Insurance Policies to Exclude War", International Business Times, Carolyn Cohn and Noor Zainab Hussain, April 8, 2022


RPSins.com

RPS RISK PLACEMENT SERVICES


The information contained herein is offered as insurance Industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis. DBA Risk Placement Services Insurance Brokers. CA License No. 0C66724.
Copyright © 2022 Risk Placement Services, Inc.