2023 Q3

Cyber Market Update

Steve Robinson
National Cyber Practice Leader

Tim Foody
Area Senior Vice President

Zach Kramer
Area Vice President

With the critical July 1 renewal cycle in the rearview mirror, we can certainly say the differences in the cyber insurance market compared to last year are striking. 2022's continuance of double- (sometimes triple) digit premium increases, limited capacity, carrier appetite restrictions and slightly downward (albeit significantly) active loss trends gave way to a different environment altogether in 2023. Building higher-limit programs was generally less challenging, and even some of the more traditionally difficult sectors attracted renewed interest from markets who, a mere year before, would have taken a hard pass.

In our last quarterly market update, we discussed the state of amnesia that tends to permeate our industry, leading to the often-predictable underwriting and rate cycles that play out. The seemingly short-lived slow down in ransomware activity, combined with the rate increases of 2020–2022, set the stage for a swift about-face in pricing and even underwriting strategy for many markets thus far in 2023.

However, continued rate reductions in the face of higher claims frequency and severity is not a formula for prolonged sustainability. Things will change—the hills and troughs that represent hard versus soft markets in cyber insurance are proving much more concentrated and steep than those demonstrated in other, more traditional lines of business, according to the Insurance Information Institute.[1] This makes sense, because the very nature of cyber risk itself is constantly changing, evolving and showing us things not previously seen. While emerging factors such as global warming will have their effects on patterns and severity of weather events, cyber is different. We will not see an entirely new, never-before seen type of fire, wind or flood that affects property policies. That's what makes cyber all the more interesting and challenging at the same time.

WIDESPREAD CYBER RISK

We have discussed in great detail the concerns insurers have with respect to widespread, catastrophic cyber risk. This risk can come in many forms, from nation-state-sponsored attacks to attacks on operating systems or software program vulnerabilities, where the chances of affecting millions of customers simultaneously is real.

May 2023 brought news of a ransomware attack that was delivered through a previously unknown vulnerability in a prominent software company's managed file transfer solution, known as MOVEit Transfer. Attribution of the attack has been assigned to a gang known as CLOP—also known as ClOp and TA505—with identified ties to Russia. Internet-facing MOVEit Transfer web applications were infected with a specific malware used by CLOP, which was then used to steal data from underlying MOVEit Transfer databases. The impact has been significant, affecting hundreds of organizations, and our carrier partners have received an inordinately high volume of claims associated with this event.

Exploits such as this are commonly known as zero days—meaning a security flaw for which the vendor of the flawed system has yet to make a patch available to affected users. The software manufacturer has long since released a patch addressing the security vulnerability in

[1] "Percent Change from Prior Year, Net Premiums Written, P/C Insurance, 1998-2022," Insurance Information Institute, accessed 21 July 2023.

the software, but not before significant effects had already been realized.

Unlike many ransomware attacks, the pattern in this attack has not been to restrict access to systems by way of encryption. Rather, they are attempting to extort their victims via a threat of release of sensitive data obtained through the exploit found in the data transfer software. The ransom amounts have typically been in the hundreds of thousands of dollars, or even in the millions for some of the larger organizations impacted. It is unclear if any have paid the ransom demand to date.

The US Department of Energy and several other government agencies, including most recently the Department of Health and Human Services[2] —along with major pension funds, banks and private businesses—have been affected by this exploit, and it is having far-reaching effects. Cybersecurity experts estimate that the MOVEit situation has affected hundreds of organizations globally, including more than 9 million motorists in Oregon and Louisiana, Johns Hopkins University, UCLA, Sony, PWC, Ernst & Young, the BBC, Shell, Putnam Investments and British Airways, among scores of others.

Insurers are wanting to minimize their exposure to widespread events that can potentially affect thousands of policyholders simultaneously. Of particular interest is the variances among different carriers' approaches to minimizing this exposure. On the extreme end, we are seeing exclusions in some cyber insurance policies specific to zero-day attacks or attacks identified as Common Vulnerabilities and Exposures (CVE), a list of publicly disclosed computer security flaws. More common, however, are exclusions that identify with more specificity, the triggers for what is considered "widespread." Events such as the MOVEit exploit would still be contemplated under coverage because it has not had, for instance, a significantly detrimental effect on the delivery of essential services to a wide population causing major societal and economic dislocation. Nevertheless, it is important that agents and brokers familiarize themselves with exclusions of this nature, work with your RPS cyber product specialist, and advise your clients accordingly.

Q3 CYBER MARKET DYNAMICS

With new events continuing to occur in the background, we are seeing mixed messages coming from the markets in response to profitability results over the past year and what is being seen as a changing risk horizon in Q4 2023 and into 2024.

Despite concerns regarding adequacy of capacity to meet the growing demand for cyber insurance, the July 1 renewal cycle, for the most part, saw fewer hurdles to getting desired capacity than in 2022. Public entity, typically among the most challenging sectors for placing coverage, showed signs of a changing market as large municipality placements previously seeing a ceiling of $20 million in capacity last year were in some cases able to make decisions on towers in excess of $50 million or higher in July of 2023.

These larger placements (with favorable loss experience) generally saw a rate decline on their primary layer. Couple this with an excess market bringing increased limit factors (ILFs) in the 70% to 85% range, and buying higher limits became an easier decision this year. As a frame of reference, many of the ILFs we saw at this time last year exceeded 100% of their primary layer pricing.

We have found retentions/deductibles to be relatively stable in the past quarter. After jarring market adjustments in 2021 and 2022 that brought significantly higher retentions, our carrier partners generally feel that retentions are where they need to be. We did not see the skyrocketing adjustments to retentions that we witnessed this time last year, when it was common to see retentions quadruple. If anything, we have seen rate adjustments for buying retentions back down in some cases—again, depending on industry sector, size of risk and loss experience.

Pricing has stabilized across the board, and as with retentions, we have not witnessed the significant increases we saw during the last renewal cycle. Renewal rates are generally flat to slightly higher in the SME sector—sub-$100 million revenue organizations—on renewals, with some even seeing rate reductions. New business has seen significant competition for acquisition of market share, particularly among some newer market entrants whose investors are not accustomed to growth rates under the 50% that they have witnessed the previous two years.

[2]The Associated Press. "The Latest Victim of the MOVEit Data Breach Is the Department of Health and Human Services", AP News, 29 June 2023.

This has led to what we view as irresponsible underwriting activity that would not have been contemplated when the ransomware epidemic was red-hot, daily, front-page news from 2019 through 2022. There is a dichotomy in play, however. Some markets, in their efforts to regain market share (or achieve it in the first place), are offering unsolicited quotes on cyber policies alongside a crime renewal, for example. Many times the coverage has been significantly restricted, or sublimits on critical insuring agreements like cyber extortion or incident response are taken down.

Tim Foody, RPS Executive Lines area senior vice president, notes, "Many markets are getting more aggressive and quoting accounts they would have declined six months ago, but they are adding exclusions and sublimits that significantly impact the coverage. There's nothing wrong with a healthy dose of skepticism toward what appears to be appetite expansion."

Further confirming the erratic nature of carrier approaches is Zach Kramer, area vice president of RPS Executive Lines who says, "Right now, I am seeing inconsistencies in underwriting not only between carriers, but also within the same underwriting teams at the same carriers. This ranges from pricing to what controls are required."

As with anything in our industry, the fine print is very important. Because each market often refers to these coverage nuances with different vernacular, it is important to partner with an expert that works in cyber insurance every day.

From a coverage perspective, rapid innovation has not been a trademark of the cyber insurance landscape since 2019. As we've opined in previous reports, there was a breakneck race for nuanced coverage expansion and buzzword add-ons in the early jostle for market share that we are not seeing now. In fact, the opposite has been in play, as carriers look to limit their exposures to third-party vendor loss, systemic risk, war and terrorism, biometric, pixel and website data collection liability exposures and increased regulatory intervention.

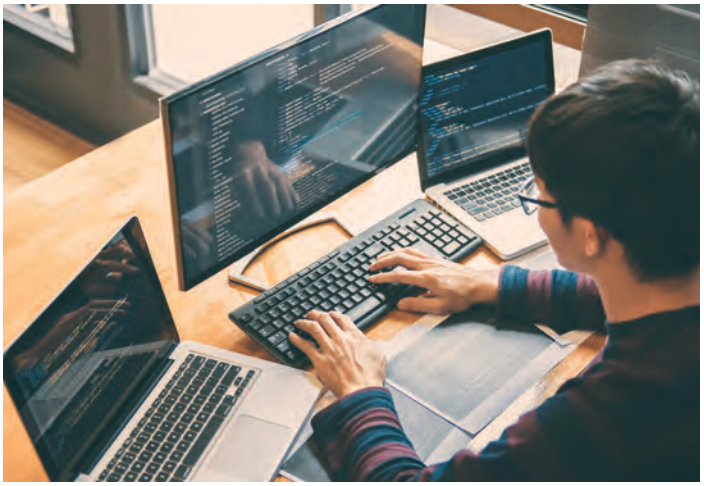
Future expansion of coverage grants will likely be implemented with precision and limited to particular industry sectors, where coverage innovation is less likely to run afoul of profitability. As a result, as is frequently the case with amendatory endorsements, there is often more sizzle than steak. Still, we see room for growth, and the RPS Cyber practice remains on the front line of coverage innovation discussions with our carrier partners, as we have been since the beginning of cyber insurance coverage.

CYBER REGULATORY TRENDS

The regulatory front remains interesting, to say the least. Nevada has recently introduced a new law, effective October 1, 2023, that prohibits defense inside the limits in liability insurance policies.[3] Many believe that while the political nature of a move like this presents benefits to consumers, the unintended consequence will likely be an exit from the market by insurers. We have had many conversations with many cyber insurers around this topic, and none are indicating willingness to leave their exposure open ended to defense of liability claims, particularly in an increasingly litigious environment around privacy matters. It will be interesting to see if lawmakers reverse course here, and if not, what the resulting fallout will be for buyers of cyber insurance policies (in addition to Errors & Omissions, Directors & Officers, etc.) in Nevada. We suspect some markets may pivot with an indemnity and first-party cyber option only—excluding coverage for defense,—but this remains to be seen.

In May, the Biden Administration announced that it's considering a ban on ransom payments as part of the International Counter Ransomware Initiative.[4] This would represent a shift in policy from previous statements made by the White House. The nuances of this possibility are complex, wrought with complications, potentially unintended consequences, and far from being settled.

Under discussion are topics such as conditions under which a waiver could be obtained allowing, for instance, organizations to pay a ransom if the threat actor is preventing access to essential services. The State of North Carolina implemented a ban on ransom payments for public sector entities in April 2022. Initial indications are that this strategy has not worked, as the number of publically reported ransomware attacks among public sector organizations have not decreased since this went into effect.



[3]"An Uncharted Frontier: Nevada First State to Prohibit Defense-Within-Limits Provisions," The National Law Review, 6 July 2023.
[4]Kapko, Mark. "White House Considers Ban on Ransom Payments, With Caveats," Cybersecurity Dive, 8 May 2023.

CYBER LOSS TRENDS

In our 2023 Q2 Cyber Market Update, we discussed potential increases in ransomware activity on the horizon, as many carrier partners were seeing a return in frequency and severity on the heels of a respite in activity of this nature in 2022 and Q1 2023. This is indeed proving to be the case, particularly in the middle market and larger insured demographics.

Our colleagues at renowned data privacy law firm Mullen Coughlin have shared that, "In 2023, through the same timeframe of January to May, there has been an increase of approximately 29% in ransomware incidents." Aligning with our predictions, Mullen Coughlin expects this upward trajectory to continue throughout the remainder of this year.

Analyzing data specific to RPS policyholders in the SME sector (sub-$100 million revenue organizations), the month of June represented a 25% increase in overall reported cyber claims. fraudulent payments and system compromise incidents led the way at 30% each. For these smaller organizations, ransomware events did not show an uptick in June, bucking the overall trend we are seeing and hearing among their larger counterparts. The MOVEit attacks were generally experienced by larger organizations, demonstrating far less impact in the SME space, explaining why the needle didn't move up in reported ransomware incidents for this demographic.

On a year-to-date basis, fraudulent payments continue to outpace other matter types by a significant margin. While the severity is far lower than ransomware, the frequency is far greater. This is creating a death-by-a-thousand-cuts effect on many cyber insurers, leading more to make adjustments to conditions-precedent wording, higher retentions and sublimits to mitigate the effect on profitability.

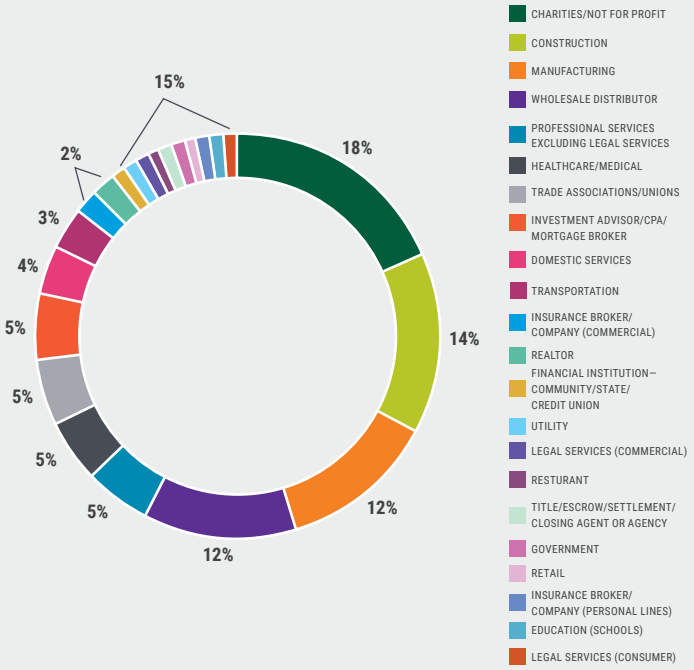
In much the same way that insurers have increasingly invested in risk management resources to help prevent data breaches and ransomware attacks, we expect to see advancements in strategies to help organizations validate changes in payment instructions in the future as well.

From an industry sector perspective, RPS small business insureds in the nonprofit, construction and manufacturing sectors lead the way in reported matters through the end of June 2023.

Information shared by Mullen Coughlin shows that their top three reported industry sectors year to date are professional services, manufacturing and distribution, healthcare and life sciences, and financial services. Business email compromise (BEC) incidents are on an all-time record pace, tracking similarly with RPS claims data (Fraudulent payment).

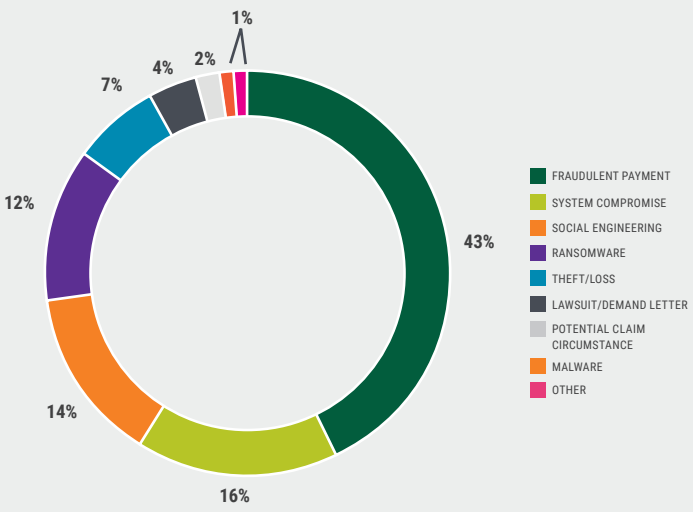
YTD CYBER INCIDENTS BY INDUSTRY

Top three are charities (18%), construction (14%) and manufacturing (12%).



YTD CYBER INCIDENT NUMBERS – SME SECTOR*

Major types are fraudulent payment (43%), system compromise (16%), social engineering (14%) and ransomware (12%).



*Source: Proprietary RPS Claims Data as of June, 2023

With all of the dialog surrounding carrier response to misrepresentation in applications and the resulting impact on claims decisions, we have a story to file in the "I thought I'd never see that happen" category. Foody says, "We had a claim that was covered, but subject to a sublimit due to controls the insured noted on the application. During the claim, it was discovered that the insured did indeed have the required control and accidentally answered the application question inaccurately. Through the RPS relationship with the insurer, we were able to have them remove the sublimit and apply the full limit to that claim. This made a massive difference in the insured's out-of-pocket costs."

THOUGHTS ON THE FUTURE

We're observing the varying approaches to a maturing cyber insurance market that different carriers are taking, with great interest. And make no mistake, there are significant differences.

As previously mentioned, rate reductions, coupled with an increase in claims frequency, followed by a relaxing of certain cybersecurity control requirements, is not a recipe for a sustainable future in this market. Thus, changes are coming.

While we don't expect the pricing shift to be as swift or severe as those experienced in 2019–2022, we expect to see increases, likely more pronounced starting in Q1 2024. We are already seeing early signs of this, but only in small pockets. New threats that creatively incorporate artificial intelligence (AI) will continue to put pressure on carrier margins, as the distribution of malware and the art of social engineering becomes more automated and widely available to those with ill intent. These new risks will also lead to innovations in prevention tactics, a race that never ends in the world of cyber risk.

Such market turbulence underscores the need to partner with experts who are adept at navigating this market and equipped with all the markets and clout to help ensure the best outcomes for your clients.

"Don't go it alone," says Foody. "This market is constantly evolving on a week to week basis, and it can be hard to keep sight on everything your clients need without a partner who is in the space all day, every day. While price is important, it's not nearly the most important consideration when comparing options."

Kramer agrees. "Bring in an expert, as most carriers are trying to limit coverage with new endorsements, and underwriters may attempt to minimize the impact these endorsements have on quotes, indicating they are not as bad as they seem," he says.

Your cyber insurance product experts at RPS are ready to help you come through for your clients in new and creative ways, giving you the confidence to focus on what you do best.

RPSins.com

RPS® RISK PLACEMENT SERVICES