Q4 2022 Cyber Insurance Market Update

The Surprises Continue

Steve Robinson
National Cyber Practice Leader

UNLIKE THE CYBER INSURANCE MARKET'S PREDICTABLE PATTERNS OF 2021 AND 2022, 2023 IS MORE APPROPRIATELY DESCRIBED AS "DYNAMIC."

If the Cyber insurance market in 2022 were to be remembered as a song lyric, the line "What a Long Strange Trip It's Been" from the Grateful Dead's *Truckin'* might be most appropriate. Brokers and underwriters new to the industry received a concentrated dose of training from both ends of the spectrum. As the year opened, the ransomware epidemic continued to churn, rates continued to rise, and capacity continued to shrink. The news of the day was usually bad and questions about market sustainability loomed. Then, things began to change.

As is always the case in cyber, old threats remained and new ones were on the horizon, but a slowdown in frequency from the number-one threat occurred. Much has been written about the reasons why ransomware attacks began to slow down. They include everything from improved baseline controls by insureds (in part driven by increased underwriting requirements to get Cyber coverage) to the war between Russia and Ukraine, forcing an entire geographic hotbed of ransomware activity to shift its focus away from American interests.

Regardless of the reasons, the fact remains that this combination of improved controls by our insureds, higher pricing, more judicious limits deployment, higher retentions, selective industry focus from our insurers and, yes, fewer claims, created a shifting market dynamic: one that suggested greater stability. At least for now.

The changes have been so stark that it is interesting to take a look back at RPS's State of the Cyber Market Quarterly Update from Q4 2021 This before-and-now chart demonstrates a few key changes over the past year.

UNDERWRITING TREND	2021 Q4 STATE OF THE CYBER MARKET	2023 Q1 STATE OF THE CYBER MARKET
Premium Trends—Primary	Premium increases 30%–150%; certain classes exceeding 400%	Premiums flat to 20%, with some decreases in the 5% range on more favorable classes; carriers are more aggressive on new business
Premium Trends—Excess	100%–120% ILF	Excess cover is easier to obtain and significantly less expensive; 65%–80% ILF
Retentions/Deductibles Trends for Middle-Market and Risk Management (RM) Clients	10x not uncommon	Stable/flat
Coinsurance	10%–50%—certain carriers—both ransomware—event-specific and across the board	New entrants to the market typically not employing coinsurance, often with a reduction in use and percent among those who previously did; application is often industry-specific

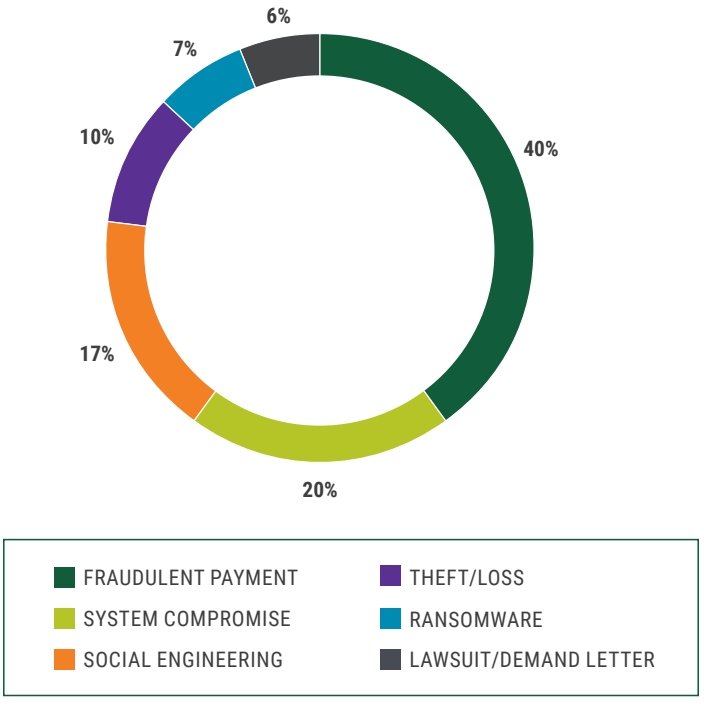
UNDERWRITING TREND	2021 Q4 STATE OF THE CYBER MARKET	2023 Q1 STATE OF THE CYBER MARKET
Systemic Risk— Event-/Exploit-Specific Exclusions	Just being introduced— Log4j, SolarWinds, Microsoft Exchange, Accellion and specific CVE rating exclusions	• Log who? • Carriers implementing new approaches to mitigating exposure to systemic risk events » Expansion of what is considered infrastructure » Easing of CVE exclusions among some markets
MFA	Required, or no coverage for vast majority of markets	Limited easing of this requirement for more favorable SME classes, but still required from all markets for middle-market and risk management accounts; some MFA vulnerabilities have been well publicized
Scans	Increased use, beyond insurtechs	Same, with a willingness to waive on SME accounts that do not have websites
War/Terrorism	Was not specifically referenced	Has become an increasingly edited coverage in light of armed conflict with Russia/Ukraine; many carriers scaling back previously wide grants of cover for electronic acts to mitigate loss when associated with a physical war between two nation-states
Reduction in Limits Deployment	$10 million limit first to go, then $5 million limit	$5 million limit coming back in limited pockets, with talk of $10 million limit coming back among a few, for favorable classes of business; still uncommon, however
Admitted vs Nonadmitted	Shift from admitted to nonadmitted, allowing for more nimbleness in premium adjustment and coverage terms and conditions	Those markets that have an admitted product are seeking a nonadmitted version as well; many that were exclusively nonadmitted filing admitted versions of their form, recognizing the demand for admitted coverage by independent agents, particularly on SME risks
Manufacturing, Construction, Wholesale Distribution, Public Entity and Education	Many markets moving away from these classes completely due to loss of frequency and severity	Restrictions largely remain, but increased underwriting in manufacturing, and understanding more closely the IT/OT relationship and protections in place allowing some room for discussion; carrier-specific

The two reports present a picture of a market that has undergone significant change in a year. We view this change as largely positive, creating a path for insurer profitability, buyer pricing stability and availability of coverage to meet the growing demand of a corporate world that recognizes the importance of Cyber insurance in their risk management portfolio. A recent corporate risk survey from Allianz[1] showed that large and small-to-midsized enterprises (SMEs) still identified cyber as their #1 threat. As a result, it's important that products are available, priced appropriately and uniquely written to cover the risks that today's businesses face.

CLAIMS TRENDS

Using the proprietary claims data that RPS collects on thousands of insureds throughout the year—primarily in the SME space—we've previously reported on the decrease in ransomware claims frequency accompanied by an uptick social engineering and fraudulent payment incidents. December's monthly reporting results, based on RPS's small to mid-sized portfolio of insureds with standalone cyber insurance coverage, kept with these trends.

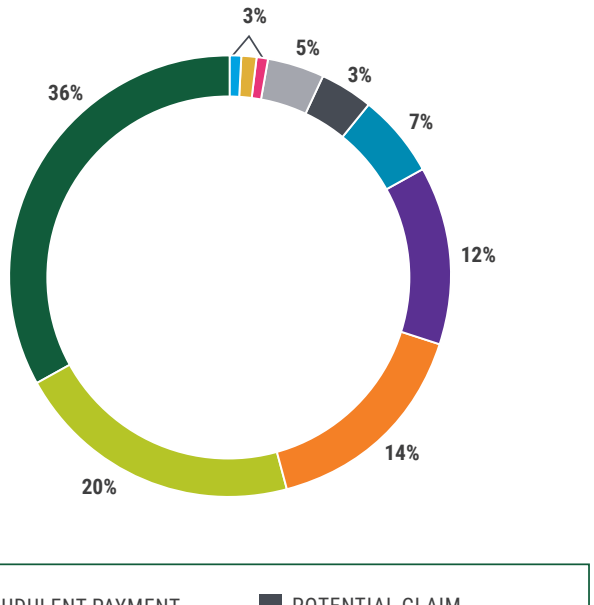
December, 2022 Claims by Matter Type— RPS SME Clients



Source: Information derived from proprietary RPS claims data among insureds in the SME sector (< $100 million annual revenue)

Ransomware events were more frequent in Q1 2022 than in the remaining three quarters, leading to the greater share of incidents for that vector on a full-year basis, as demonstrated below.

Calendar Year 2022 Claims by Matter Type— RPS SME Clients



Source: Information derived from proprietary RPS claims data among insureds in the SME sector (< $100 million annual revenue)

While ransomware frequency has dropped, these events certainly haven't gone away. Of particular interest is our front-row view to ransomware attacks today versus the view we had in prior years. For instance, in November 2022, a US school district experienced a significant ransomware attack that completely shut down classes for three consecutive days. Thanks to strong leadership and significant investments made in the cybersecurity infrastructure by the board of education, this story ended much better than it would have two years earlier.

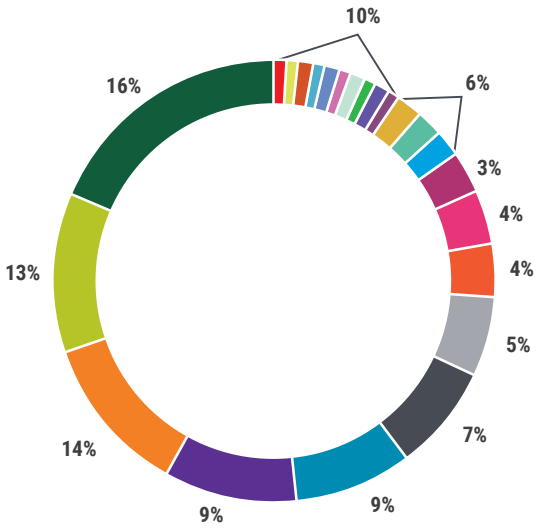
The district didn't pay the ransom demand and instead was able to restore their networks from reliable backups that were physically separated from the affected systems. That's not to say that expenses weren't incurred to deal with the outage.

Even with the most up-to-date backup procedures and dedicated internal resources working with highly capable, insurer-provided incident-response vendors, expenses will still exceed $250,000.

This story is a perfect example of how the right combination of a well-prepared insured, partnering with an informed and responsive broker and the expert resources available to them via their cyber insurance policy, can make an extremely disruptive event manageable and even affordable.

From an industry perspective, due to the wide array of industry classes insured, it's more useful to look at the full-year claims results, rather than a monthly snapshot.

Calendar Year 2022 Claims by Industry Type— RPS SME Clients



Source: Information derived from proprietary RPS claims data among insureds in the SME sector (< $100 million annual revenue)

In 2022, we began to see a slight increase in third-party claims associated with Illinois Biometric Information Privacy Act (BIPA) and the Telephone Consumer Protection Act (TCPA). It will be interesting to monitor third-party claims in the developing regulatory landscape that 2023 will continue to bring.

REGULATORY LANDSCAPE

As reported by JD Supra,[2] January 2023 ushered in new privacy laws in five states: California Privacy Rights Act (CPRA), effective January 1, 2023; the Virginia Consumer Data Protection Act ("Virginia Act"), effective January 1, 2023; The Colorado Privacy Act ("Colorado Act"), effective July 1, 2023; The Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("Connecticut Act"), effective July 1, 2023; and The Utah Privacy Act ("Utah Act"), effective December 1, 2023.

Generally, these state laws give consumers the rights to delete and access data, rights to opt out of targeted advertising and non-discrimination rights for exercising these rights. The new laws also provide enforcement bodies, including the new California Privacy Protection Agency (CPPA), with resources and authority to enforce the laws. Only California provides a private right of action for consumers in the event of a data breach. Overall, 2023 will see increased regulatory activity in the privacy space.

From a federal perspective, the American Data Privacy and Protection Act (ADPPA) was the first federal online privacy bill to pass committee (House Energy and Commerce) by a vote of 53-2 on July 20, 2022. The bill was intended to regulate how businesses use and store consumer data and provides additional rights to consumers. However, even with bipartisan support, the bill has yet to pass and faces opposition from various legislators who cite enforcement concerns.

At the time of this report, it is too early to tell if the new requirements CPRA imposes will lead to increased third-party litigation as newly created CPPA delayed issuance of final rules. These rules will likely be released in late January 2023, with existing regulations remaining in effect for the time being.

CYBER INSURANCE CAPACITY

The year has started with market news relative to cyber insurance capacity and how it's deployed. Beazley launched what it described as the global reinsurance market's first cyber catastrophe bond, reports Insurance Journal.[3] The bond provides Beazley with "indemnity against all perils in excess of a $300 million catastrophic event, with the potential for additional tranches to be released through 2023 and beyond." The bond is backed by a panel of insurance-linked securities investors and signals new and creative deployment of capital in an effort to enable the cyber insurance market to grow as demand continues to increase.

Another sign of movement in the cyber insurance marketplace have been demonstrated by both Chubb and Crum & Forester deciding to drop their former quota share arrangements, instead opting to retain their portfolios on a net basis, employing excess of loss coverage to further hedge their positions. It's expected that insurers will continue to drive rate, although in a far more measured fashion than in the previous two years. We're seeing this fluctuate from carrier to carrier, also impacted by industry sector and size of risk.

WHAT CAN AGENTS AND THEIR INSUREDS EXPECT IN 2023?

Unlike the predictable patterns of 2021 and 2022 that delivered drastically increased rates, intense underwriting scrutiny, shrinking capacity and a skittish approach from new entrants, the theme of 2023 is more appropriately described as "dynamic." Solid, predictable patterns haven't yet shown themselves, as carriers are taking varying approaches to profitably growing their Cyber coverage portfolios in the New Year. We're seeing everything from premium reductions and an easing of the strictest underwriting requirements from 2022 for some small businesses to a continuance of the discipline applied last year, in an effort to establish longer-term profitability on books of business that had taken a significant hit since the rise of ransomware attacks. Inconsistency is perhaps the most consistent adjective we can use right now.

In our last market update, we reported that some markets have very short memories, and we continue to see this demonstrated for certain placements. There's great pressure for new business as investors are looking for top-line growth, particularly among some in the insurtech space. This pressure has shown itself through a willingness to ease certain security control requirements among smaller insureds, particularly in more loss-averse sectors.

The good news is, insurers appear better prepared to withstand losses, should ransomware activity return to more 2021 and Q2 2022 levels. After all, data suggests that insureds are better defended, recovery capabilities have been improved, and insurers generally have less exposure to the more frequently attacked industry classes.

Agents can expect to receive more proactively generated Cyber insurance quotes from admitted markets that tapped the brakes during the more high-profile loss years. As you once again begin to receive Cyber quotes automatically on crime renewals when you didn't ask for them and low-cost "cyber" endorsements on package policies, be careful. These products will likely bear little resemblance to the ones you might have received in 2020. Industry losses since that time have necessitated significant changes in terms and conditions, the increased use of sub-limits and additional fine print that you may not be accustomed to looking for. Navigating a Cyber insurance claim for your client is not the time to discover these nuanced changes.

Now, more than ever, it's imperative that you work with a specialist in the field of Cyber insurance. The twists and turns of the last three years have provided great insight to those who place Cyber policies day in and day out. For those agents getting back in, you'll find that the environment is different and always changing. With specialized market insight, a large team of Cyber insurance professionals throughout the US and proprietary insurance products, RPS is well prepared to help you come through for your clients.

Sources

[1]"Allianz Risk Barometer 2023," Allianz, 2023. PDF file.

[2]Augustinos, Theodore and Alexander Cox, "U.S. State Privacy Laws in 2023: California, Colorado, Connecticut, Utah and Virginia," JD Supra, 14 Dec 2022.

[3] "Beazley Launches Global Re/insurance Market's First Cyber Catastrophe Bond," Insurance Journal, 9 Jan 2023.

RPSins.com

RPS® RISK PLACEMENT SERVICES