2023 Q2

Cyber Market Update

Steve Robinson
National Cyber Practice Leader

Entering the second quarter of 2023, the cyber insurance market continues to mature rapidly, showing new and sometimes conflicting patterns, seemingly daily.

The insurance industry has often been accused of having a short memory. Perhaps in no other sector are market cycles predicted with more certainty. Yet the very factors that take us into challenging markets are often followed by periods of amnesia, leaving agents, brokers and insureds scratching their heads.

Case in point: The years were 2020 to 2022. The rise of ransomware, coupled with an environment of poor security controls, contributed to a rash of cyber insurance claims that forced a hard and fast market correction. Loss ratios had quickly deteriorated and something had to be done. Insurers dramatically increased rates, reduced limits, increased retentions and required more stringent IT protections—like multifactor authentication (MFA)—to help shore up the vulnerabilities that led to ransomware attacks.

As a result, ransomware frequency dropped, and profitability returned to the fastest-growing sector in insurance. Certainly, other important factors such as the war in Ukraine, a fully remote workforce returning to the office, and higher government and law enforcement focus contributed to these improved results as well. However, the most significant levers of rate, exposure and barriers to entry were pulled with great force.

So what does every new insurance market cycle do in the face of prosperity? Naturally, the opposite of what got us there to begin with. So far in Q2 2023, we're seeing great disparities among insurers as they seek growth without the benefit of rapidly rising renewal rates.

Among the strategies currently employed are:

- Rate reductions, which are significantly more pronounced on middle market and large risks
- A walk-back on requirements for certain IT controls in more favorable industry classes, specific to small to midsize enterprises (SMEs)
- Expanded appetites for industry classes previously considered out of bounds
- A return to $5 million limit offerings for more insureds, previously limited to $2 million or $3 million, with some markets offering $10 million once again
- Easing of risk scoring thresholds to qualify for insurability and more favorable terms
- Significantly reduced pricing for excess cyber—inverted increased limit factors (ILFs) from 2022 as low as 65% for the best risks

Having said that, it's important to note that carriers aren't employing these strategies consistently, making this maturing market all the more unpredictable.

RANSOMWARE HASN'T DIED

In our last quarterly cyber market update, we discussed the decrease in ransomware frequency and how fraudulent payments had taken over the top position in claims frequency. While this trend still holds in Q2, it's not to say that ransomware has gone away. What we are seeing is a significant drop in an organization's willingness to pay. Forensic and cyber extortion incident response firm Coveware reports a dramatic drop, showing that 85% of ransomware victims paid the ransom in Q1 of 2019 versus 37% in Q4 of 2020.[1]

RPS has observed similar trends on our own book, but from an insurance perspective. And even with this drop in propensity to pay, significant costs of forensics, data restoration, legal advice and business interruption costs persist. These factors make every ransomware attack, regardless of whether the threat actor is paid, an extremely taxing event causing significant financial, operational and reputational impacts to those affected.

We've noticed, and corroborated with several insurers in the past 30 days, a marked increase in ransomware activity in April. After a very light February and a slight increase in March, it's still too early to tell if this is a trend that will continue. However, a variant known as Royal has shown significantly increased persistence. These threat actors focus primarily on critical infrastructure sectors including manufacturing, communications, healthcare and public healthcare, and education, according to the Cybersecurity & Infrastructure Security Agency? (CISA).[2]

Recently, one of our insureds experienced a Royal ransomware attack and was left with no option other than to pay, as its backups were unknowingly housed in the same environment as the primary network.

Just last week, a law enforcement agency became the most recent victim of Royal, forced to respond to an initial demand of nearly $2 million. Its cloud backups weren't secured. Unlike the insured mentioned above that will suffer operational disruption and inconvenience, the impact on law enforcement or healthcare organizations can carry life-threatening consequences. In this case, officers in the field cannot communicate with dispatchers at headquarters.

CISA's Cybersecurity Advisory suggests the following high-level actions for mitigating cyberthreats from ransomware:[2]

- Prioritize remediating known vulnerabilities that have been exploited.
- Train users to recognize and report phishing attempts.
- Enable and enforce MFA.

From a recovery perspective, regular backups of an insured's critical data are among the most important steps to avoid paying a ransom. The backups should be completely isolated from the network, either stored off-site and encrypted or stored in the cloud with separate access credentials. If backups are remote, use MFA to protect access and test backups regularly to ensure their efficacy.

THIRD-PARTY LIABILITY CLAIMS ON THE RISE

As state and federal privacy laws continue to expand their scope, and as the confluence of technology, media and advertising become more intertwined in an organization's daily operations, we're witnessing a significant impact on third-party privacy claims.

Remember that part of a cyber insurance policy that you don't pay a lot of attention to, because your insureds mainly want the "red phone" to respond to their information security emergencies? Now you're more likely to see the liability side of the policy triggered than ever before, and insurers are taking measures to limit their exposure to these lower-frequency, higher-severity claims on their books.

Leading the way in third-party liability claims this quarter are incidents involving the unauthorized collection of web data, specifically using website trackers, pixels and cookies.

Lokker, a business intelligence software and big data analytics platform, summarizes the "why" of this new phenomenon quite well in a recent report:

"According to HTTP Archive's latest Annual State of the Web Report (September 2022), 94% of sites use at least one third party and, on average, the top 1,000 websites use 53 third-party scripts including ads, analytics, CDNs, chatbots, video delivery services, content providers and social media features. Introducing all this activity into millions of browser sessions has become mayhem for unauthorized data collection, theft and exploitation. Thus, the customer's web browser is now a hotbed of cyber risk, exposing visitors to malware, theft of their private information and violations of privacy laws."[3]

What does this mean from a cyber insurance perspective? Insurers are taking swift action to avoid costly privacy litigation claims in their policy wordings. Many carriers are relying on broad unauthorized collection and use exclusions in their policies to avoid paying defense costs and indemnity for claims of this nature. Some are applying sublimits, while others are increasingly introducing specific pixel-tracking exclusions, particularly in the healthcare space (for example, a hospital patient portal collects data and shares it with a social media platform in an effort to target patients for medical devices, medications or other services that could directly treat the patient's condition).

Data suggests that merely incorporating the use of such tools in an organization's privacy policy online isn't sufficient. We expect these lawsuits to continue expanding among organizations in varying industries, including retail and hospitality.

Insurers are increasingly using URL-scanning technologies and additional questionnaires to underwrite around this risk. Agents and brokers should familiarize themselves with this trend, and search policy forms and endorsements for exclusions relative to wrongful or unauthorized collection, pixel-tracking and similar wordings. Advise your insureds of their potential exposure in this area, and today's cyber insurance policies likely won't cover claims of this nature. You can point them to resources that can help them assess their risk, such as free web-based pixel-scanning technologies like Blacklight.[4]

Cyber insurer Beazley suggests the following as a start:[5]

- Take an enterprise view of risk and compliance growing your business and engaging with customers in the digital space.
- Ensure that legal and risk teams work with marketing to see what technology marketing is, and how they are collecting, using and retaining data for targeted advertising.
- Liaise with third-party marketing agencies to understand data collection and contracts.
- If your company chooses to use pixels despite the risk, engage an outside privacy expert to help determine how to place the pixels on your websites and to craft notice/consents that can help minimize liability.

DATA INTEGRITY THREATENS CLAIMS ADJUDICATION

Chronologically speaking, the big shift in cyber insurance underwriting occurred roughly two years ago. It was then that acronyms such as MFA, EDR, SEG and IRP found their way into the daily vernacular of cyber specialty underwriters and brokers. This increasingly technical view of risk left many retail insurance agents confused at best, not to mention the small businesses they insured.

Particularly in the SME sector—where businesses often lacked sophisticated in-house IT resources—the prospect of completing an application for cyber insurance became daunting. Facing a firming market with much higher barriers to entry, their answers in cyber insurance applications often didn't reflect the true view of risk in insureds' IT systems. Likely more often unintentional than deliberate, the inaccuracies were now in the insurance underwriting ecosystem, and only the future would tell the impact this could have.

Fast-forward to today. As organizations experience the usual cyber-related incidents that affect everyone, insurers and brokers are increasingly finding themselves in uncomfortable conversations when adjudicating claims for their clients. When the fact patterns of a claim don't agree with what was represented on an application, the disconnect can potentially lead to claim denials—not a spot anyone wants to be in. While misrepresentation has been a factor to deal with since the very origins of insurance, the highly technical nature of cyber underwriting has created an environment where the risk is now much higher. The fact is, many of the scanning technologies insurers use today can't assess some of the more important technologies insurers require for cyber insurance eligibility. As a result, they still rely on accurate information in paper applications.

We expect two trends to gain traction in the current effort to more effectively underwrite cyber risk, avoiding the aforementioned conflicts.

- Insurers increasingly are offering discounts for organizations that agree to let underwriters past the front door. We call this digital validation. Taking IT security assessments beyond perimeter scans to now observe the environment behind the firewall is a much more accurate way of assessing risk. Not surprisingly, organizations are often reticent to open a view into their systems for fear of not only an increased threat to their security, but also a perceived negative impact on insurance coverage available to them when their safeguards don't meet the exacting standards of underwriting

- Conditions precedents in cyber insurance policies will expand. In much the same way that many insurers require dual-authentication attempts before authorizing changes in payment instructions for social engineering coverage, we'll see similar tactics with respect to segmented backups, the use of MFA and other security tools in the policy wording itself.

The short story here is this: Insurers are less interested in using their funds as the sole risk transfer tool for small businesses. For coverage to apply, insurers will increasingly require at least the most basic prevention measures to be in place. Wanting to avoid bad faith claims at all costs, insurers may wish to more frequently incorporate these requirements into the policy language itself. By not merely relying on accurate answers in applications—and leaving the nuances of the absence of words like "any" and "all" to dictate coverage applicability—insurers will begin to feel more comfortable that their coverage offerings are in line with their risk assessments.

Time will tell how often and to what extent insurers will incorporate strategies like digital validation and condition precedent policy wording to reduce their risk. One thing is for sure, the old phrase "trust but verify" will describe cyber underwriting in the future. Agents and brokers are wise to closely review cyber insurance applications with their customers before submitting them to brokers and insurers. As these applications become more nuanced, so too can the impact of their answers on coverage in the policies. Make all best attempts to verify the accuracy of these answers before a conflict arises.

CLAIMS TRENDS

In our last state-of-the-market report, we began sharing RPS-specific claims data on our insureds, particularly in the SME sector. Using the data on thousands of cyber insurance clients and more than 1,000 claims, not only can we tell that ransomware claims still occur, we can tell you that they've been experienced most in charities/nonprofits, manufacturing, construction, wholesale distribution, government and healthcare.

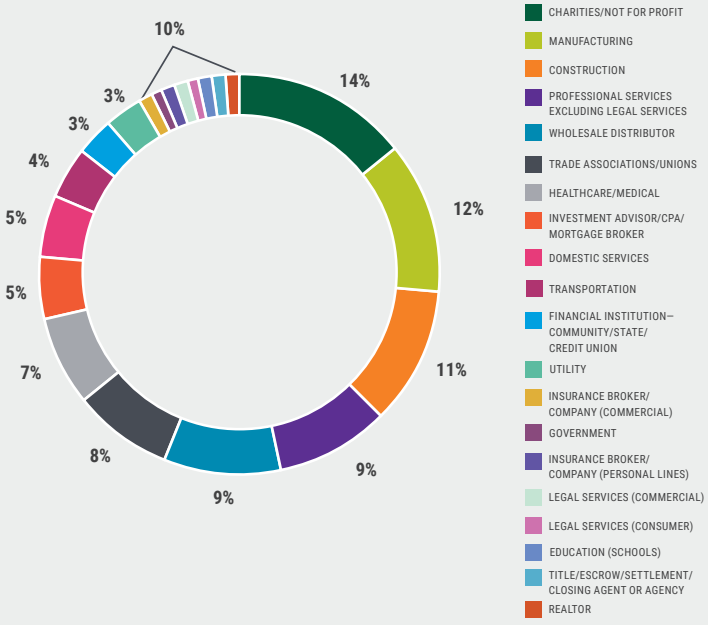
We observe that, for instance, more incidents occur in March than May, and that healthcare experiences their biggest spikes in the month of September. The average ransom demand among our SME clients in March was just over $300,000, and the average paid (among those who did pay) was $192,000. The average fraudulent payment trended lower in March at $35,000. Having real-time actionable data like this allows RPS to more accurately structure the most appropriate cyber insurance programs for our retail agents and our mutual clients.

Here are some updates on the claims front after the first three months of 2023, based on information derived from proprietary RPS claims data among SME insureds with less than $100 million annual revenue.

While March saw an uptick in new matters versus February, claims volume remains slower, relative to historic norms, and industry types affected by claims were more evenly spread, with no one industry dominating.

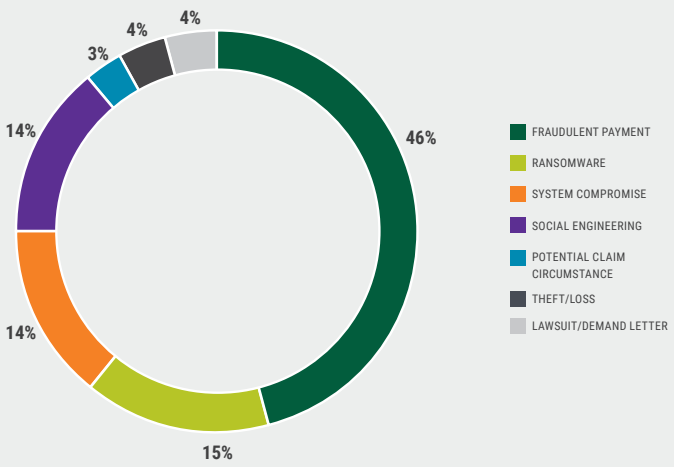
YTD CYBER INCIDENTS BY INDUSTRY

Top three are charities (14%), manufacturing (12%) and construction (11%).



YTD CYBER INCIDENTS BY MATTER TYPE

Major types are fraudulent payment (48%), ransomware (15%), system compromise (14%) and social engineering (14%).



REGULATORY ENVIRONMENT CONTINUES TO EVOLVE

There continues to be movement among states to expand laws protecting consumer privacy. In our last report, we touched on the state laws in various stages of change in California, Colorado, Connecticut, Utah and Virginia. In addition, some existing federal laws are expanding, such as the protections afforded under Gramm-Leach-Bliley and new requirements for financial institutions to protect the security of customer information. These requirements don't stop with the traditional view of financial institutions, but extend to peripheral entities that act in similar capacities—such as car dealerships—where the collection of sensitive financial and personal data is extensive.

To underscore points made earlier about inconsistencies among carrier approaches to cyber insurance and a distribution system that's confused by the rules, in February, US Senators John Hickenlooper and Shelley Moore Capito introduced the Insure Cybersecurity Act. This bipartisan legislation aims "to protect consumers and small businesses against cyberattacks by providing clearer information surrounding cyber insurance policies." The bill aims to create a "dedicated working group to develop recommendations for issuers, agents, brokers and customers to improve communication over cybersecurity insurance coverage levels."[6]

WAR AND CYBER WAR POLICY LANGUAGE CONTINUES TO DEVELOP

Since Lloyd's introduced its model clauses for cyber war and cyber operation exclusions in November of 2021, much development has taken place in this area—both among Lloyd's syndicates and domestic US insurers.[7] While their approaches differ, one thing is certain: Cyber insurance policies were never intended to cover, nor were they priced for, cyber events in conjunction with a physical war that has a wide lateral affect, felt by a significant population.

The problem is that these new exclusions can show themselves in two basic forms:

- An expansion of cover under former war exclusions, providing more clarity and high thresholds for applicability
- A restriction of cover, when excluding for acts of sovereign states, not tempered by a requirement that the attack is a part of a wider-scale effort that causes significant harm to the functioning of the affected state
- It's important that agents read the fine print and understand the potential impact to their insureds who have concerns about how these unlikely yet devastating events could affect their coverage.

LOOKING AHEAD

In an industry experiencing such a rapid rate of change, it's important for agents and brokers to be closer to their clients than ever. For cyber insurance, it's likely that your renewal conversations will be much more pleasant than the ones you had this time last year. With a more stable market and excess liability coverage now offered at a significant value, you should be discussing higher limits where warranted.

If you're unsure what constitutes "warranted," we recommend consulting a broker who specializes in cyber insurance. Also, as more insurers are get in the game after two years on the sidelines, beware of unsolicited cyber insurance quotes that might accompany ancillary lines on your renewals. Without close review, you may find that their new approach to the market could include significant coverage restrictions compared to markets who have weathered the storm.

With broad market representation and tens of thousands of cyber insurance customers in all 50 US states, RPS stands ready to assist you and your clients for what's possible.

Sources

[1]"Improved Security and Backups Result in Record Low Number of Ransomware Payments," Coveware, 19 Jan 2023.

[2]"#StopRansomware: Royal Ransomware,"Cybersecurity & Infrastructure Security Administration, 2 Mar 2023.

[3]Fisher, Kaitlyn. "Online Data Privacy Report—March 2023," Lokker, 7 Mar 2023.

[4]Mattu, Surya. "Blacklight," The Markup, accessed 24 Apr 2023.

[5]Heaton, Katherine. "Cyber Risk Revealed: Pixels and Tracking Technology," Beazley, 14 Dec 2022.

[6]"Hickenlooper, Capito Introduce Bill to Help Better Insure Small Businesses Against Cyber Attacks," US Senator John Hickenlooper, 21 Feb 2023.

[7]"Cyber War and Cyber Operation Exclusion Clauses," Lloyd's Market Association Bulletin, 25 Nov 2021.

Optional related articles

1. https://www.rpsins.com/learn/2022/dec/five-trends-you-need-to-know-about-in-the-cyber-market/
2. https://www.rpsins.com/learn/2022/nov/how-to-navigate-your-next-cyber-renewal/
3. https://www.rpsins.com/learn/2022/nov/2023-us-cyber-market-outlook/