WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 67, Issue 11 Thursday, March 16, 2023

GUEST COLUMN: Cyber Risk Report: What to Expect in 2023

By: Matthew Thomson, Director of Cyber Liability; Alex Friedl, Brokerage & Cyber Liability Account Executive; and Megan Peyton, Cyber-Brokerage Account Manager, M3 Insurance, WHA's Premier Partner

Every organization faces cybersecurity risks that could reveal sensitive information and wreak havoc on their business continuity plans. For large corporations and the public sector, this doesn't come as a surprise, but even small businesses should be aware of evolving cyber risk and the market's response to increasing cyber-attacks.

M3's director of cyber liability Matt Thomson was quoted in the *Milwaukee Business Journal's* Table of Experts, saying, "The first mistake is thinking you don't have anything cyber criminals want."

Matt Thompson, Alex Friedl, and Megan Peyton, M3 Insurance

In this report, M3's cyber leaders break down what cyber-attacks were most common in 2022, which cybercrime tactics are emerging as threats in 2023, and how the cyber liability market is reacting to criminals' new methods with shifts in underwriting and new ancillary services.

2022: The Hard Market Plateaus

The hard market for cyber insurance began in 2019 due to an explosion in the frequency and severity of ransomware claims. Thankfully, policyholders received a reprieve in late 2022 after years of brutal rate increases and coverage reductions.

The reason for the plateau in the market is two-fold: a combination of rate increases and decreases in claims paid.

Carriers measure their profitability by comparing the premium taken into their expenses, which are primarily in the form of claims. The math is relatively simple: as higher rates and reduced claims began to take effect, the profitability of carriers' cyber books increased.

Why Were There Reduced Cyber Claims in 2022?

There are two main reasons for the reduction in cyber claims. First, the number of ransomware attacks dropped precipitously at the same time as the Russian invasion of Ukraine. (I) It is presumed that the war is related to the reduction the frequency in ransomware attacks, as many ransomware groups are based in former Soviet Bloc countries.

Ransomware attacks were also less severe in 2022 due to improved cyber controls.

In Q1 of 2019, 85% of ransomware victims needed to pay the ransom. By Q4 of 2022, that figure was reduced to 37%.

Coveware, an incident response firm that specializes in ransomware, postulated that improved backup procedures are the main reason for the decrease in ransoms paid. (II) If an organization has secure back-ups, then they can restore from their backups rather than having to pay the ransom to obtain the decryption key.

Common Cyber-Attack Methods in 2022

Cybercriminals continued to get creative in 2022. Organizations of every size can learn from the frequently used tactics highlighted below when working with their broker to create a cyber risk management strategy.

Last year, "MFA bombing" became a popular method of bypassing multi-factor authentication, which is one of the best tools for preventing unauthorized network access. Two high-profile breaches at Uber and Rockstar occurred back-to-back in late

2022. In both of these instances, an 18-year-old hacker named Tea Pot used social engineering to obtain login credentials from employees of these organizations. Then, Tea Pot sent repeated multi-factor authentication prompts to the victims until they became frustrated and finally accepted a prompt, which provided Tea Pot with access to Uber's and Rockstar's networks. (III)[I]

It is important that security professionals stress the importance of declining and reporting unexpected multi-factor authentication prompts, as "MFA fatigue" remains a risk. Learn more about MFA fatigue from M3's Director of Cyber Liability Matt Thomson.

Beazley, one of the largest cyber insurance carriers, tracks ransomware vectors as seen in their claim intake.

- **The leading vector for ransomware attacks in Q4 2022 was Remote Desktop Protocol (RDP).** It is absolutely critical that any externally facing RDP ports are secured by multi-factor authentication.
- **Phishing also remained a common ransomware attack vector in 2022**. Regular phishing simulations, and remedial training for those who fail, are important controls for minimizing the human factor that continues to befuddle cybersecurity experts. Phishing training will also help reduce fraudulent instructions claims, also called social engineering, which have risen across all industries in 2022. While not as severe as ransomware claims, fraudulent instructions claims are the most common claims we see. (IV)

Cyber carriers are typically not willing to offer more than $250,000 in limit for cyber-crime coverage, so it is very important to have robust risk management procedures, as much of the risk is uninsurable. We recommend working with a broker who has dedicated cyber risk management experience to protect your organization, your employees, and your data.

Systematic risk
Systematic risk became a hot button issue in 2022 as cyber insurers grappled with their reinsurance renewals. Reinsurers were concerned about their exposure to catastrophic cyber events such as cyber war and dependent business income losses.

The former is relatively clear, and Lloyd's of London mandated that their syndicates clarify that the war exclusion applies to cyber war.

The latter is regarding major vendors such as Amazon's cloud service, AWS. If AWS were to go down nationwide, the dependent business income losses for policyholders could be catastrophic. Most carriers put out endorsements limiting coverage for these catastrophic events.

In 2023, we have seen carriers begin to separate the dependent business interruption risks from the war risks. Many carriers, especially on high premium policies, have become more flexible on the war exclusion wording, which is more in the spirit of the original Lloyd's bulletin.

What Do We Expect In 2023?

The Cyber Market is Splitting
In late 2022 and early 2023, we have seen a split in the cyber market. Risks with no claims and superior cyber controls are seeing rate increases in the neighborhood of 0% to 15%. This is wonderful news for policyholders that suffered through 50% to 100% rate increases for the past couple of years. We expect this rate plateau to continue for accounts that carriers view as good risks.

On the other hand, risks with substandard controls or severe claims will experience an entirely different market with higher rates, reduced capacity, and coverage limitations. Limiting coverage for ransomware and cyber extortion continues to be a favorite tactic of carriers for accounts they view as particularly risky.

Technology is Supporting Underwriting Intensity
The underwriting intensity that began in the hard market will continue into 2023. After years of minimal underwriting, carriers began to require much stronger controls as their profitability crumbled in the era of ransomware. Each carrier has their own proprietary ransomware applications, and the applications became more intricate in the latter stages of the hard market.

We have not seen any relaxation in underwriting requirements, nor do we expect to see any in 2023. Carriers still view good controls as critical to managing the risk in their book of business, but they are willing to be flexible on accounts with good controls and no claims.

Underwriting tools to be aware of
External scanning will continue to be popular in 2023. Many carriers, particularly the start-up MGAs, have turned to these non-intrusive scans as one of their primary underwriting tools. With these scans, carriers can view vulnerabilities as a threat actor would, and either decline to quote or require that the vulnerabilities be remediated prior to binding coverage.

Another underwriting tool that is being beta-tested is "inside out underwriting". While scans are currently externally facing, there are

several companies that are working on tools that would provide carriers internal access to a risk's network for more accurate underwriting.

For example, the policyholder would provide the insurance carrier access to their cloud system so the carrier could view the security settings. This is analogous to personal auto policyholders downloading a mobile app that adjusts their premium based on how they drive.

The big question is whether security professionals are willing to give carriers this access. For many CISOs, the potential rate reduction is not worth the intrusiveness of this underwriting technique.

Greater Offerings from Carriers
We expect to see carriers continue to offer ancillary services that improve the security controls of potential policyholders. One of the biggest obstacles to carriers growing their book of cyber business is that many of the submissions they receive do not have adequate security controls. Carriers are attempting to tackle this obstacle in a few ways.

A large American insurance company is partnering with a firm that will assist potential clients implement multi-factor authentication, so more risks fit within their appetite.

Other start-up companies are taking a more radical approach. One example is a start-up that is both an insurer and a provider of cybersecurity services. They offer their own security products such as endpoint detection and response, multi-factor authentication, and offline backups. The combined cyber insurance and cyber security suite is a wonderful fit for businesses that feel overwhelmed when trying to meet underwriting requirements.

Predicted Cyber-Attack Methods in 2023
It is tough to say whether the reduction in ransomware attacks will continue into the rest of 2023, or if it will turn out to be a temporary lull.

The war in Ukraine will continue to have implications on the frequency of cyber-attacks. Currently, Eastern European ransomware groups are preoccupied with the conflict in Ukraine. For example, a Russian threat actor could have been drafted into the infantry and there are not many opportunities to conduct ransomware attacks in a remote outpost in the frontlines of Ukraine.

If the war ends, we expect to see an uptick in cyber-attacks as these individuals will be free from their government service and will be able to direct their energies towards criminal pursuits. Additionally, Ukraine and Russia could turn to ransomware as a funding mechanism to rebuild their countries after years of war.

The MGA dilemma
While MGAs (managing general agents) are not new, they have multiplied in recent years. MGAs are like carriers in that they can issue quotes, bind coverage, and administer claims, however they have a less robust balance sheet and rely heavily on reinsurance.

This puts insurance brokers and buyers in a tough position. Often, we are faced with two quotes, one from an MGA and one from a traditional insurance carrier. The MGA quote may have similar or better coverage to the traditional carrier in addition to a lower price.

Which one should you buy? The lower premium quote from a less financially stable MGA or a more expensive quote from a traditional carrier with ample reserves? This question can only be answered by the buyer depending on your price sensitivity and risk tolerance.

In Conclusion
In 2023, we expect a continued stratification of the cyber market as good risks will continue to experience the benefits of a softer market, while substandard risks will struggle to find adequate coverage. Technology will be a driving factor in this stratification. Carriers will develop and utilize tools to both analyze risk when quoting and help potential policyholders meet their underwriting criteria.

The future of ransomware is murkier and will depend on how the conflict in Ukraine plays out. In the long-term, we expect the frequency of ransomware attacks to ramp up as the war winds down, but the severity will depend on the results of the cat-and-mouse game between security professionals and threat actors. Hopefully, the severity will plateau as organizations continue to focus energy and resources on their cybersecurity.

M3's cyber team continues to monitor the cyber liability market, as well as evolving threats to cybersecurity. Reach out to your M3 account executive to discuss how the market impacts you, and which risk management controls you should put in place to protect your organization, employees, and data.

Sources

[I] arcticwolf.com
[II] coveware.com
[III] avertium.com
[Iv] beazley.com
[v] beazley.com

Other Articles in this Issue

- GUEST COLUMN: Industry Voices—Let's be Transparent About Hospital Price Transparency
- As Drug Costs and PhRMA Profits Soar, New National Alliance Forms to Threaten 340B
- Republican Lawmakers Announce Legislation Providing New Exceptions to Wisconsin's 1849 Abortion Law
- Advocate Health's Carlson Recognized with WHA 2022 Distinguished Service Award
- WHA Celebrates National Patient Safety Awareness Week: March 12 -18, 2023
- GUEST COLUMN: Cyber Risk Report: What to Expect in 2023
- Sen. Marklein Asks Hospital Leaders to "Keep Me Educated"