PRISM
Public Risk Innovation, Solutions, and Management

February 15, 2023

To: PRISM Cyber Program Members

From: Gina Dean, CEO

Re: Stakeholder Message PRISM Cyber Program Members

Better Together - It's still a good time to be in a JPA!

The cyber insurance industry is in a mixed market cycle, which is impacting every cyber insurance carrier and insured across all sectors. The market is mixed because it is neither fully in a hard market or soft market cycle, as is commonplace for insurance. It's in a cycle where poor risks, whether it is security controls or losses or a combination of both, are experiencing a continuation of the hard market. Good and best in class risks are seeing a more favorable marketplace where coverage may be expanded and premiums and rates may experience flat renewals or lower increases. For risks that have the security controls in place and good loss history, the hard market cycle seems to be tempering. For risks that have poor security controls and/or unfavorable loss history, the hard market cycle is continuing. As PRISM members begin their budgeting process, I want to take this opportunity to provide some background information on the state of the market and the status of the PRISM Cyber Program.

Background

The cyber insurance market has shifted considerably in the last 24 - 36 months and is presumed to continue to be volatile for the foreseeable future. The top 10 carriers, who control an estimated 65%-75% of the U.S. standalone insurance market, have been overwhelmed with cyber incident claims, and have found a temporary normal to operate in, which includes more rate and tighter scrutiny on security controls of their insureds. Ransomware, social engineering/business email compromise, attacks on organizations with systemic reach and other attacks have left no class of business immune to the attacks.

The large increase in the severity of claims has been driven by many factors, including our continued dependence on technology and digitization, globalization, the size of the ransoms being demanded and paid, as well as business interruption and system rebuilding costs. The norm three to four years ago was for ransoms to be tens to hundreds of thousands of dollars. In the past six months, however we have seen the demand for public entity ransom payments reach over $10M.

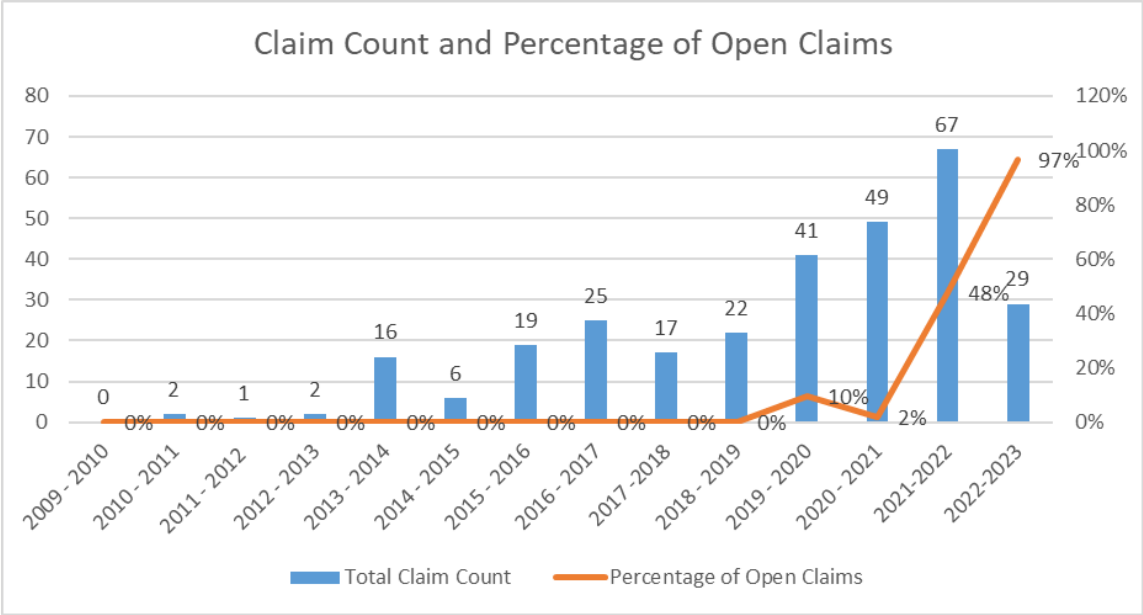
Public entities continue to be a large and frequent target for hackers for several reasons: 1) IT infrastructure and training budgets for public entities are still generally smaller than their commercial counterparts; and 2) Public entities are seen as a vulnerable target due to the necessary services provided to the general public.

Because of the increase in frequency and severity of claims, cyber insurers are requesting more underwriting information, requiring more senior level oversight, increasing premiums dramatically, and reducing capacity/appetite in all sectors, most notably for large public entities.

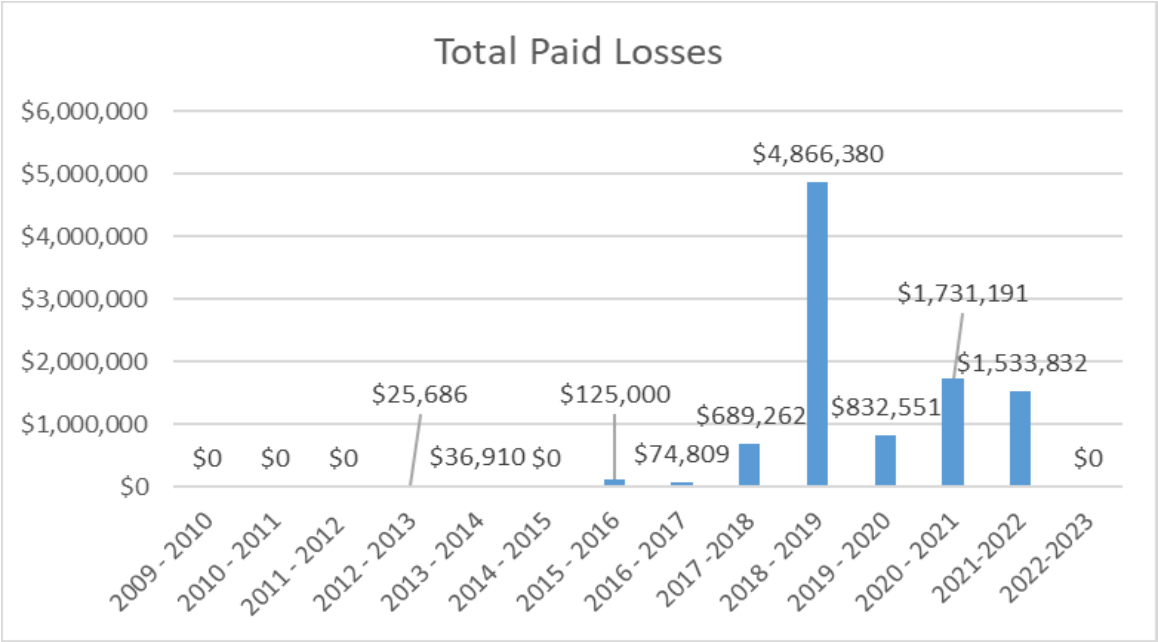
In 2023, however we are seeing more capacity come into the marketplace in terms of private equity, public company raising of capital, new insurance linked securities in Bermuda, and other capital infusions. This is contributing to a slight easing on premium increases for good risks and an increased appetite to write public entities. Alliant has provided our submission to Beazley, our incumbent provider, and will also be marketing our program to multiple insurers for the renewal of the PRISM Cyber Program. We expect the sentiment towards the public entity sector in the cyber insurance marketplace to be more favorable than it has in the past two years, for good risks. If this is the case, it may translate into more favorable or stable coverage, either in the form of sub-limits, increased limits, stable retentions, and/or less volatility in premium changes.

As all of the aforementioned affects the insurance industry, they also affect PRISM. We continue to experience both frequency and severity of claims in the program. The following two graphs depict the frequency and severity of claims by PRISM members over the last 14 years.

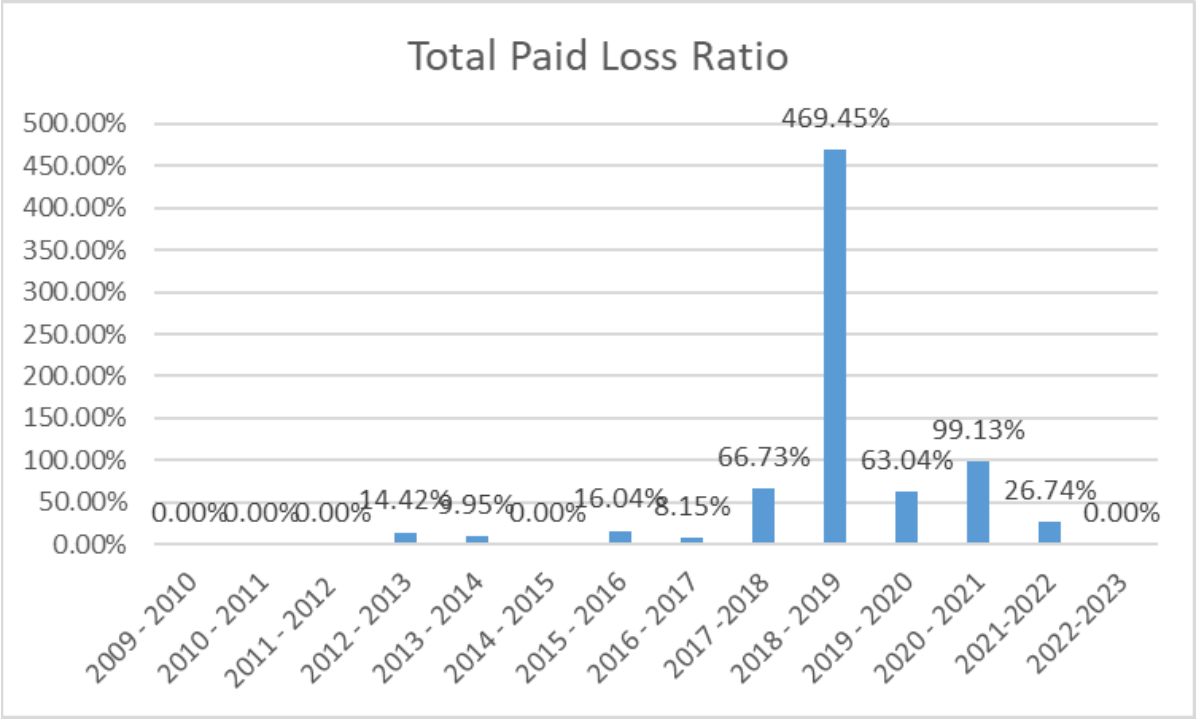
The first graph highlights the fact that until four years ago, the frequency of cyber claims is what you would expect as a “normal” trend; however, the significant increase in frequency since 2019, was certainly unforeseen by the industry.



The second graph highlights the uptick in severity over the past six years. It also shows how volatile losses in cyber insurance can be, and that any year can have losses which are multiple times larger than any historical losses seen by the Program.



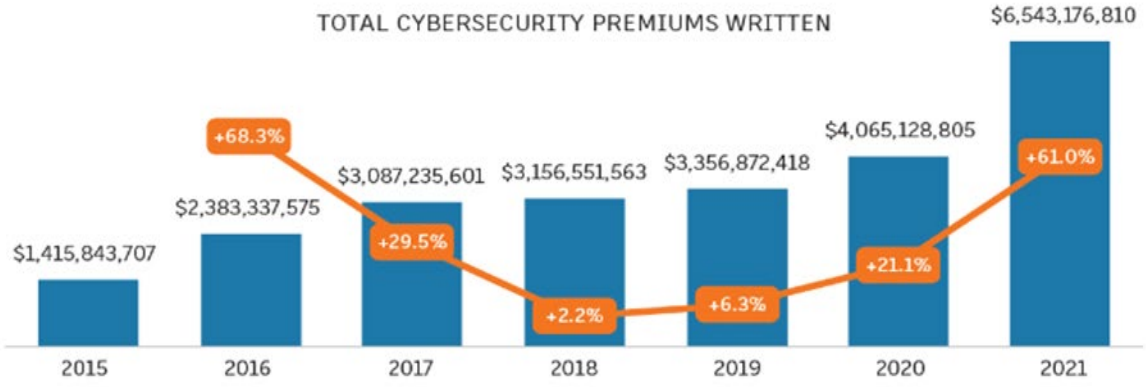
In addition to the increases in claims frequency and severity, the following graph highlights the increase in the paid and projected loss ratios of claims in the PRISM Cyber Program over the last 14 years. Again, the graph highlights the uptick in loss ratios, which changed significantly starting five years ago, with 2021 and 2022 too early to determine where loss ratios may end up.



The following two graphs depict the written premium, demand and claims in the general U.S. cyber insurance marketplace. The graphs are from the National Association of Insurance Commissioners and the Council of Insurance Agents and Brokers, which exhibit many industry trends including the rise of premium, demand and claims. An item of note is the insurance company repositioning, meaning there was a lot of reshuffling in their portfolios to understand the risk they have on hand and how they will move forward.

CYBER INSURANCE MARKET*

The total U.S. market for cybersecurity insurance increased 61.0% to $6.5 billion in 2021 from $4.1 billion in 2020.



*U.S. domiciled insurers and alien surplus lines insurers

LARGEST CYBER INSURERS

The top 10 U.S. groups wrote 57.4% of the cyber insurance, totaling $2.8 billion in 2021.

2021 rank	2020 rank	Company	Direct written premium	Market share
1	1	Chubb Ltd.	$473,073,308	9.8%
2	8	Fairfax Financial Holdings Ltd.	$436,447,801	9.0%
3	2	Axa Insurance Group	$421,013,729	8.7%
4	11	Tokio Marine Holdings Inc.	$249,785,218	5.2%
5	3	American International Group Inc.	$240,613,748	5.0%
6	NR	Travelers Cos. Inc.	$232,276,831	4.8%
7	5	Beazley Insurance Co. Inc	$200,877,555	4.2%
8	7	CNA Financial Corp.	$181,382,785	3.8%
9	NR	Arch Capital Group Ltd.	$171,944,995	3.6%
10	6	Axis Capital Holdings Ltd.	$159,059,212	3.3%

Source: National Association of Insurance Commissioners

Safety in Numbers

Thankfully for members of the PRISM Cyber Program, our size offers economies of scale that could not be realized without being in a pool. In the hard market we were able to leverage our volume to benefit all Program members and we continue to use this leverage in the mixed market. The amount of increase for individual members is dependent upon your entity's claims experience and size. If you are one of the lucky ones who have not yet experienced this new reality in claim trends, you may expect to see increases, but to a lesser degree. The PRISM Committees and Board of Directors have dedicated time and resources to ensure premiums are equitable amongst the members, based on an allocation that takes into consideration each individual member's potential exposure *and* claims experience.

The Big Picture

If we have learned from history, we know that joint powers authorities (pooling) have been the answer to turbulent markets. By staying the course, we have weathered the hard market together, and we will continue to benefit from our economies of scale and our sharing of best practices to help manage risk and hard markets.

While PRISM's premiums may increase for 2023/2024 policy year, the premiums have still been less costly than an entity would be faced with outside of the pool. We will continue to navigate, test and push the markets to maintain the benefits the members have seen in the PRISM Cyber Program.

Member's Response

In October, 2022 the PRISM Executive Committee approved a policy directing members of the Cyber Program to participate in a Cyber Security Health Check once every three years. This was done in an effort to help members manage cyber risk and be aware of best practices in this very specific area of risk management. The cost of this service is covered by the PRISM Cyber Program.

PRISM has contracted with its longstanding business partner Synoptek, to assist in the implementation of this initiative. The Health Check process is facilitated by cyber security experts from Synoptek and consists of the following:

1. A one-hour interview (teleconference) with a Synoptek representative to gain an understanding of the organization's current cyber security controls
2. A subsequent one-hour overview (teleconference) with a Synoptek representative to review findings and recommendations for program maturity
3. A comprehensive written report with findings and recommendations

To help get the most from this service, it is critical that a representative with a working knowledge of cyber security controls participate in this process. PRISM will begin working with Synoptek and members to begin scheduling these assessments shortly.

Additionally, there are several other actions that should be taken during these continued, turbulent times:

1. Communicate the state of the market to all of your stakeholders, so there is an understanding that this is industry-wide.
2. The severity of claims is on the rise. Please consider ongoing cyber security training for staff, as well as strengthening your cyber security practices and systems. PRISM has partnered with Knowbe4 to deliver an engaging cyber security training program at exclusive discounted rates.
3. Anticipate an increase in your own SIR funding.
4. Fill out an application on the Alliant Cyber Public Entity Application Portal.
5. Have an incident response plan in place, as well as a dedicated incident response colleague or team.
6. Work very closely with your insurance claims manager during a claim, and obtain agreements made during the process from the insurance carrier in writing.
7. Ensure you are working with the insurance company's paneled vendors, to maximize claim expertise, sublimits, and the depth/breadth of your coverage.
8. Continue to engage PRISM on risk assessments and stay up to date on other risk control tools/information available to the membership.

Finally, manage your individual risk by taking advantage of the best practices programs and service partner programs PRISM offers.

As always, if you have questions or need additional information to better understand the current environment or to communicate to your internal management and governing officials, please let us know.