PRISM
Public Risk Innovation, Solutions, and Management

April 6, 2021

To: **PRISM Cyber Program Members**
From: **Gina Dean, CEO**
Re: **Stakeholder Message PRISM Cyber Program Members**

This memorandum is to inform the members of the PRISM Cyber Program ("Program") of the current cyber insurance marketplace, how this affects the Program, and a general view of program loss activity and marketing efforts.

The cyber insurance industry is in a hard market cycle, which is impacting every cyber insurance carrier and insured across the nation, across all sectors, and now especially it is affecting public entities. 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. Also attached are talking points and an information sheet that we hope you will find useful in communicating to your stakeholders.

Background

The cyber insurance market has shifted considerably in the last 12-18 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, are being overwhelmed with cyber incident claims. SolarWinds, Microsoft Exchange, and other attacks have left no class of business immune to the attacks.

The large increase in the severity of claims is driven by the size of the ransoms being demanded and paid, as well as business interruption and system rebuilding costs. The norm, 18 to 24 months ago, was for ransoms to be tens to hundreds of thousands of dollars. The new norm is in excess of a million dollars. Public entities are a large and frequent target for hackers, for several reasons. The IT infrastructure and training budgets for public entities are generally smaller than their commercial counterparts. Public entities are seen as a vulnerable target due to the necessary services provided to the general public.

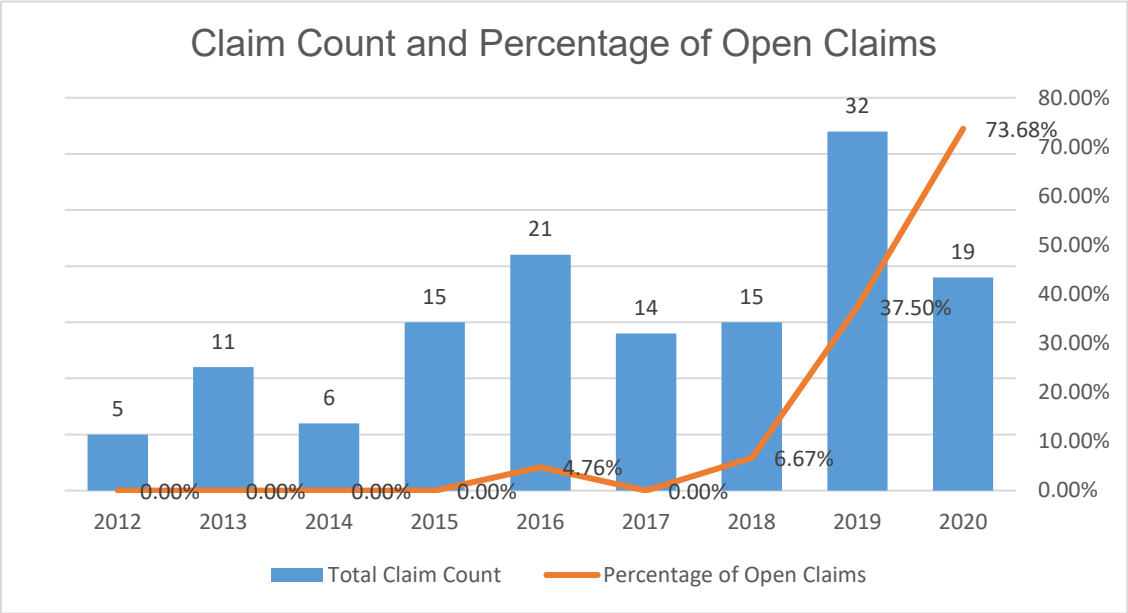
Program losses are one of many factors driving premium and structure changes for this renewal. Cyber insurers are requesting more underwriting information, requiring more senior level oversight, increasing premiums dramatically, and reducing capacity/appetite in all sectors, most notably for large public entities.

Our broker, Alliant, reached out to 50 insurers for the renewal of the PRISM Cyber Program; 47 markets declined the primary layer without any further discussion due to lack of appetite for the public entity sector and two are pending a response. The one market that is willing to quote is the incumbent, Beazley. Their pricing and coverage changes;

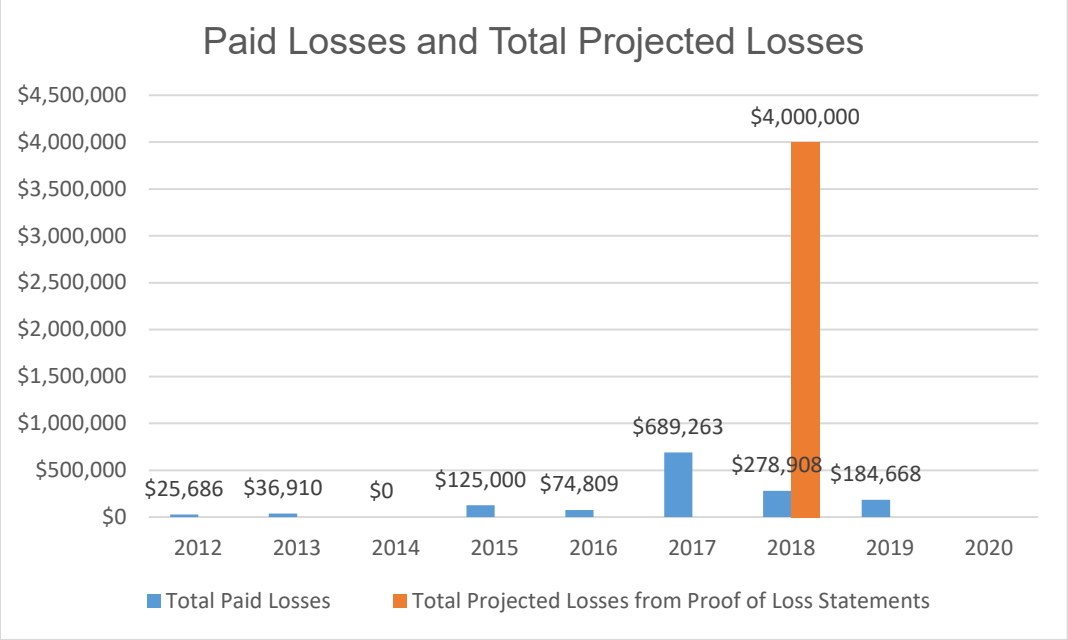
however, reflect the sentiment towards the public entity sector in the cyber insurance marketplace. More and more we are seeing coverage modifications either in the form of sub-limits, reduced limits, higher retentions, and/or material increases in premiums. At the same time and for the same reasons, self-insured and pooled programs across the state are seeing a depletion in funding. This trend is affecting all public entities: counties, cities, schools, and special districts.

As these issues affect the insurance industry, they also affect PRISM. We are experiencing an issue of both frequency and severity of claims. The following two graphs depict the frequency and severity of claims by PRISM over the last 9 years.

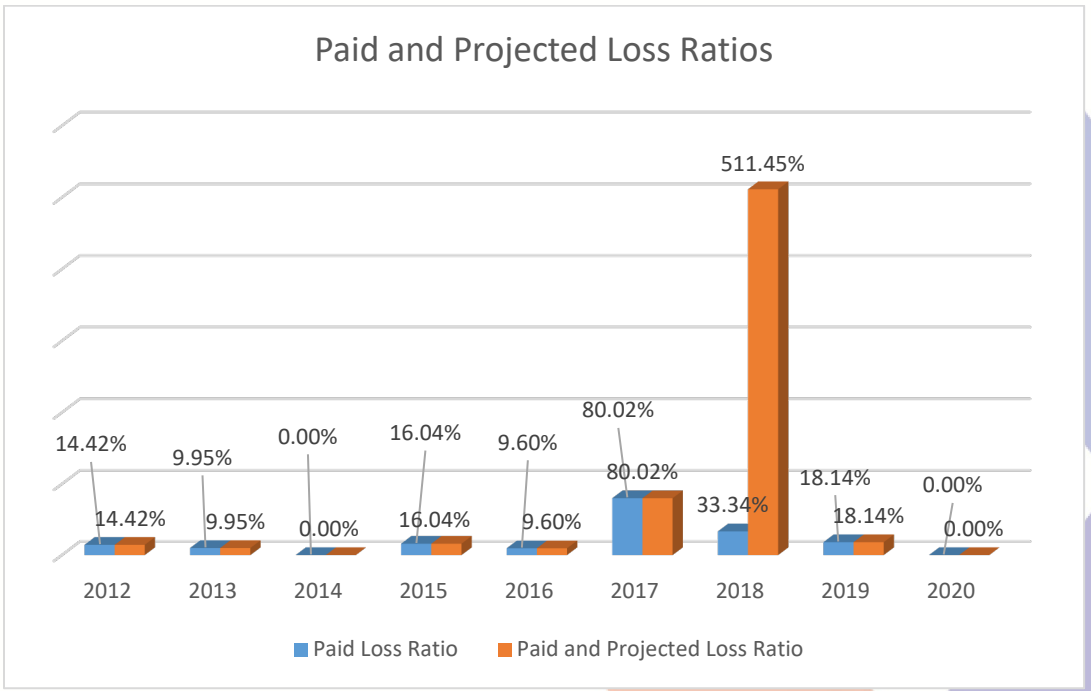
The first graph highlights the fact that until two years ago, the frequency of claims is what you would expect as a "normal" trend; however, the significant increase in frequency since 2019, was certainly unforeseen by the industry.



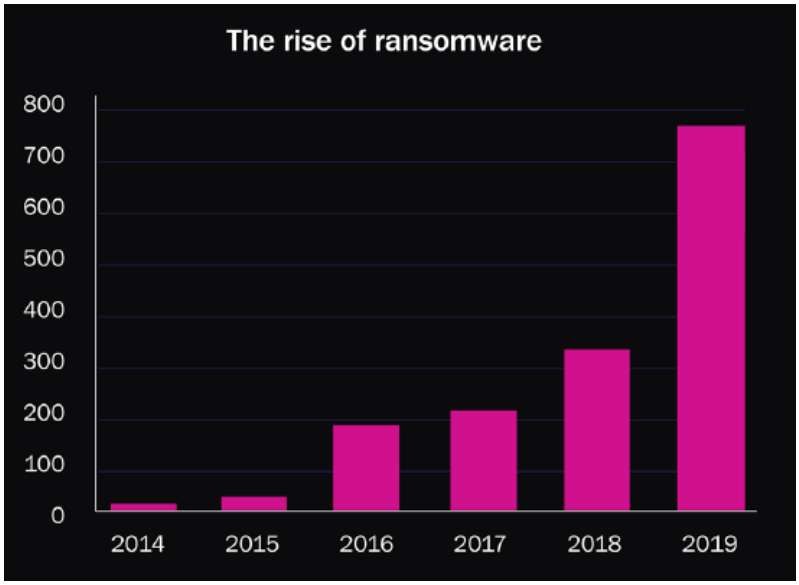
The second graph highlights the uptick in severity over the past 3 to 4 years. It also shows how volatile losses in cyber insurance can be, and that any year can have losses which are multiple times larger than any historical losses seen by the Program.

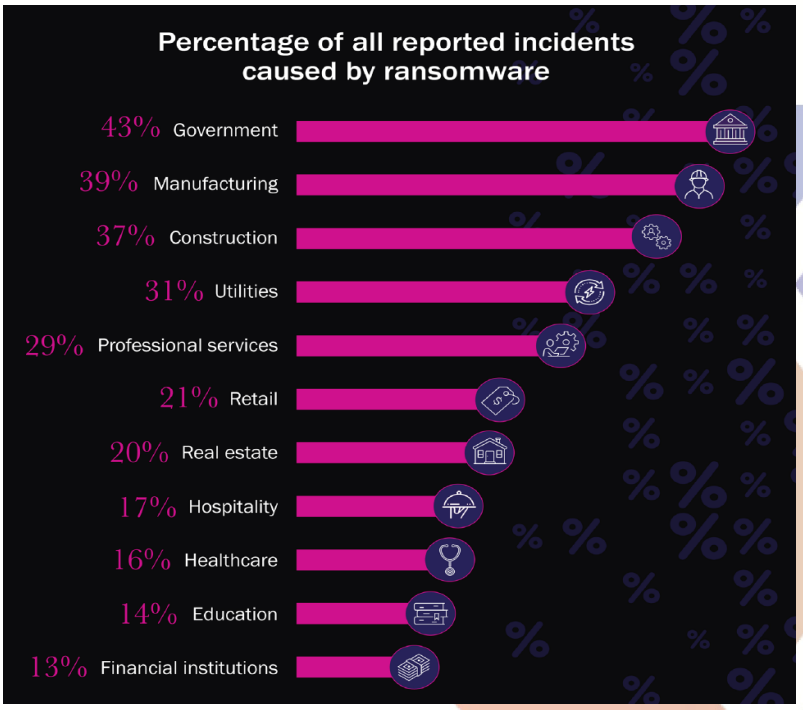


In addition to the increases in claims frequency and severity, the following graph highlights the increase in the paid and projected loss ratios of claims in the PRISM Cyber Program over the last 9 years. Again, the graph highlights the uptick in loss ratios, which changed significantly starting 4 years ago, with 2019 and 2020 too early to determine where loss ratios may end up.



Two final graphs depict ransomware claims in the general marketplace. The graphs are from the 2020 Beazley Breach Briefing, which discusses many industry trends including the rise of ransomware claims and the percentage of reported ransomware incidents by industry sector. Note that governmental agencies are at the top of the list. Overall, the graphs show ransomware claims have doubled from 2018 to 2019, with cyber extortion claims comprising of 43% of all reported claims for governmental entities in the dataset.





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. We are able to leverage the volume we bring to the markets to benefit all Program members.

That being said, the PRISM Cyber Program will see extraordinary rate increases this year, which are a reflection of our own losses and of the 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 can expect to see extraordinary 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 will all benefit from our economies of scale and our sharing of best practices to help manage risk and hard markets.

While PRISM's premiums will increase for 2021/2022 policy year, the premiums are still less costly than an entity would likely be faced with outside of PRISM. We have spoken with 10 markets on various sized members, with losses and without, to test the PRISM Cyber Program pricing and competitiveness. Of the members tested, we requested indications for $7M to $12M in limits. The results were 37.5% of the members received full declinations, and 62.5% received indication ranges for limits of $2M to $5M. There were no indications provided for over $5M in limits, even when requested. The lowest premium indication received for $2M in limits and $75k in retention for the smallest member in the group marketed was $17,000. The largest member in the group marketed received an indication of $180k for structure of $2M in limits and a $1M retention. All pricing indications we received in this marketing effort are non-bindable without a full review of a cyber application and ransomware supplement, with the potential of additional underwriting information being requested.

Member's Response

There are several steps that can be taken during these turbulent times:

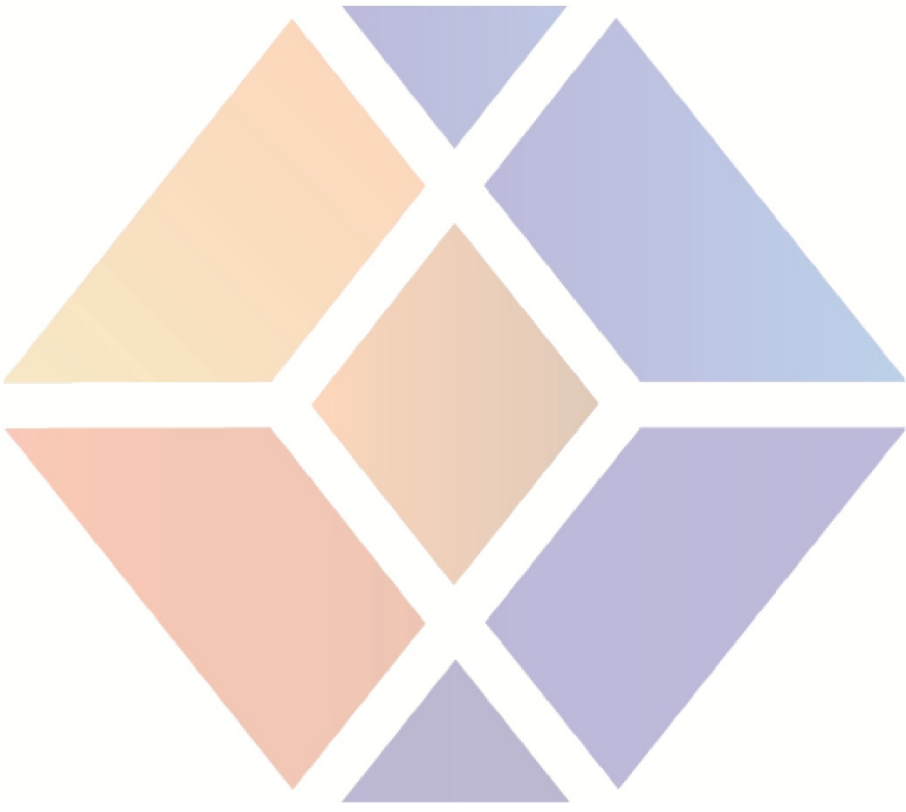
1. First, communicate the state of the market to all of your stakeholders, so there is an understanding that this is an industry-wide problem.
2. The severity of claims is on the rise. Please consider ongoing cyber security training for staff, as well as strengthening your cyber security

practices and systems.

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. PRISM is creating a cyber-risk self-assessment tool to assist members evaluate their program. More information will follow once developed.

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.



Talking Points for the PRISM Cyber Program

Individual Claim Examples

	Member A	Member B	Member C	Member D
What Happened	A single lost unencrypted laptop	Ransomware attack	Ransomware attack. Core clinical server, pharmacy, lab, electronic records all breached. Hospital system admins were able to quickly shut the systems down and restored most everything because of well-kept backups.	Ransomware attack. Minor incident. No ransom paid
Coverage Parts Affected	100% Breach Response	Breach response as well as 3rd party claim for data network liability	Breach response as well as Business Interruption claim	Data Restoration Costs
Size of Claim	$400k Total $300k for doc review $50k for legal $50k notification costs 9k notified lives	$500k Total in breach response $300k for computer forensics $100k legal Unknown size of claim for third party liability	$100k Total for breach response $50k legal $50k forensics $2M proof of loss submitted for BI	Did not breach retention
Lessons Learned	Make sure all workstations and mobile equipment are encrypted	Forensics revealed that no health data was breached so no notifications were required and the insured is facing a 3rd party class action suit regardless. Lesson is that healthcare faces the threat of a class action suit even if data is not breached	Patient data was encrypted and wasn't accessed. 100 hospital employees had information accessed. Large complicated claims can have a long tail	If concerned with retention, please fund adequately, as retentions are increasing in this marketplace

Claims Trends

- PRISM tracks loss development for all the program years. In the years 2017 and 2018 the claims severity has spiked, with 2018 being the worse year since the inception of the Program. While in 2019 and 2020, the frequency increased, with severity to be determined, since cyber insurance is now becoming a longer tail line of business with the type of claims shifting.
- The natural result of this significant change in losses is that PRISM has adjusted forecasts and rates to account for new loss trends, as have our carriers. We continue to anticipate extraordinary rate increases to reflect the increased claims costs.

Benefits of Being in a Pool

Economies of scale benefits

- Historical access to insurance options. PRISM's size historically provided more leverage in the insurance market via premium volume, which has helped PRISM secure a unique cyber program 10 years ago and maintain relationships with market leading carriers.

Long Standing Relationship in Cyber Insurance Marketplace

- Because of PRISM's foresight to start a cyber insurance program a decade ago, with one of the top leaders in the cyber insurance marketplace, the Program now benefits from a material and positive relationship with the most senior underwriters at Beazley. The ability to obtain a quote in the most turbulent cyber insurance market in the history of this line of business is largely based on PRISM's continuous partnership with Beazley. Beazley is seen as a market leader in the space, and their continued partnership with PRISM is vital to our marketing efforts for the excess insurance layers.

Equitability

- PRISM's members with large loss experience continue to have coverage and premium options in the pool, which would likely be difficult to obtain or not available at all depending on the size of the loss. Members with less severe loss experience also receive benefits from pooling as they are not charged market based premium, large minimum premiums, and obtain similar coverage the Program has historically provided. At the moment, carriers in the cyber insurance space are beginning to exclude key coverages associated with ransomware incidents.
- PRISM's premium allocation is equitable, including a surcharge for members who impact pool rates with large claims to offset increasing costs for members who are not contributing large claims.

General Market Information

- The cyber insurance market continues to harden. We continue to see a significant increase in ransomware incidents and demands, contributing to high dollar claims.
- Claims trends have affected PRISM, just as they have affected the industry.
- Markets continue to be more judicious with how and where they deploy their capacity and/or limit their exposure. Market capacity is very limited for the public entity sector, especially large public entities, JPAs/pools, and entities with large losses. Many markets are also only writing excess cyber insurance and excluding key coverages associated with ransomware incidents.

- The severity of claims in the Program have increased with several above $500k, and one limit loss for the primary layer. This is a big indication cyber incidents are increasing and are increasingly more expensive.
- We have always been proactive in our management and approach to making funding decisions, and this remains the same today. Members can expect substantial pool rate increases for 2021/22.
- The benefits of pooling shine brightest during a hard market when our economies of scale, our historical leverage with markets, our long standing relationships, and our sharing of best practices help manage risk.