Insurance Resolution: Preparing for Cyber Claims

By: Tim Schotke, Chad Anderson, John Blatt

Introduction

Cybersecurity insurance ("Cyber") is a rapidly growing, relatively immature segment currently making industry headlines for emerging risks and high-stakes coverage disputes. Cyber introduces new challenges from the resolution perspective. The uniqueness of these claims calls for a specialized approach for Cyber carriers, from regulation to resolution.

While many Cyber *Liability* policies may simply reimburse for business interruption or other losses after the fact, other Cyber insurance products promise a full suite of legal, technological and regulatorily-mandated services to policyholders. Such products differ from the property and casualty policies normally handled by P&C receivers and guaranty funds which consist almost exclusively of payments for losses. For coverage to be in any way effective, it is essential that specialized services such as legal breach coaching and digital forensic analysis be delivered to the policyholder within minutes or hours of an incident being reported, rather than days or weeks.

A regulator or receiver stepping into a troubled Cyber writer may not have any experience taking in these claims and interfacing with this unfamiliar class of vendors. When such a company is liquidated, affected guaranty funds may not be prepared to expedite coverage determinations and may not have access to the information needed to process Cyber claims.

The purpose of this paper is to identify areas where the resolution system must work together to ensure an adequate level of pre-liquidation planning. Doing so will ensure that both receivers and guaranty associations are prepared when a Cyber insurance carrier enters the system. Whatever the challenges, we share a responsibility to ensure protection is delivered to the policyholders in a meaningful timeframe.

Background

Cyber insurance is growing rapidly both in the amount of coverage in force and in the number and cost of claims. The NAIC's September 12, 2019 Report on the Cybersecurity and Identity Theft Insurance Coverage Supplement (appended) indicates that for those companies that completed the Supplement to the P&C Annual Statement in 2018, approximately 500 insurance companies were selling Cyber coverage, with just over $2 billion in 2018 premiums. This is up slightly from $1.89 billion in 2017 premiums. Cyber coverage is sold as a stand-alone policy, as a bundled coverage, or as an endorsement or rider attached to an underlying insurance policy. When including premiums from endorsements and riders, the total premium for the Cyber market is much higher, at roughly $3.6 billion. This number has increased each year with no signs of slowing down.

A typical standalone Cyber policy is a complex product that provides services to policyholders in addition to payments for losses. Companies vary in the products they offer, with some allowing the policyholder to develop a customized bundle of coverage from a comprehensive menu of offerings. Elements of a Cyber policy can include:

- Claim Management – first-party costs for legal, forensic, public relations and other claims costs;
- Security & Privacy – third-party liability coverage for damages, mandatory costs, and legal defense;
- Ransom & Extortion – Ransomware and similar risks (somewhat similar to a kidnapping and ransom policy), which may include securing a ransom payment in the form of cryptocurrency;
- Business/Network Interruption;
- Regulatory – cost of compliance with public investigations and state data breach notification requirements; and
- Specialty – which includes D&O and E&O coverage, among other things.

Standardized Cyber policy language is not in use, and the policy language being used by those insurers with a lower degree of experience and expertise may not have been given adequate analysis with respect to such emerging risks as "silent coverage". Silent coverage, or "non-affirmative cyber", is the concept of losses not excluded by policy language, but potentially not anticipated by underwriters or factored into premium and coverage decisions. Policy exclusions are evolving quickly but, like the policy forms themselves, so far have not been standardized across the industry to the authors' knowledge. Given the absence of standardized policy language, there is consequently the absence of a large, shared historical experience database to assist companies in underwriting and accurately pricing these products.

Financial Reporting

Clear financial reporting of Cyber exposure by companies is necessary for insurance regulators, receivers and guaranty funds to prepare themselves to handle Cyber claims. It is our understanding that no uniform direction exists for reporting Cyber premiums to regulators on the Exhibit of Premiums and Losses within the P&C Annual Statements. While we presume that standalone Cyber policies may most often be reported as General Liability, an endorsement to a preexisting policy is potentially reported in the same line as the underlying policy (perhaps as Medical Malpractice premium, as discussed below). Although regulators and receivers have greater access to confidential company information, guaranty funds typically do not have access to that information pre-liquidation and must refer to publicly available information and court filings at the time public proceedings begin against the troubled carrier. The lack of a dedicated reporting line or field for Cyber premiums written makes it difficult for funds to determine whether a company wrote Cyber insurance. For example, Galen Insurance Company sold Cyber coverage as a rider to their Medical Malpractice policies. Because these endorsements were not distinct from the primary polices on publicly available documents, there was no advance notice to the guaranty funds of any Cyber exposure.

Regulators overseeing troubled companies may want to pay particular attention to those that are selling Cyber for any of the reasons above. However, the varied methods of issuing

Cyber coverage may present challenges for regulators in deriving an accurate aggregation of all the Cyber risk assumed by a particular insurer. The aggregate risk challenge also has implications for premium reporting and solvency regulation. The Exhibit of Premiums and Losses requires insurers to report premiums by line of business and is supplemented by certain interrogatories. Currently, it may be comparitively difficult for regulators to develop a holistic measure of a given insurer's exposure to Cyber risk. The lack of easily accessible measures of overall Cyber exposure may also hinder the ability of receivers to quickly assess the risks the company presents. Further, guaranty funds are unable to accurately predict their funding, staffing and vendor needs in the face of a possible liquidation if Cyber coverage is involved.

The entire insurance resolution system would benefit from improved transparency regarding individual carriers' Cyber exposure. When a company becomes troubled, interrogatory responses could perhaps be combined with public information and shared with the guaranty funds pursuant to a confidentiality agreement, which would help ensure the funds are properly prepared for any potential Cyber claims.

Enhanced Tools for Examiners

Financial examiners are the early investigators of a troubled company. When financial examiners are in the early stages of investigating a company, it may be beneficial for them to assess the true scope of the Cyber exposure for that company. Currently, the NAIC's Financial Condition Examiners Handbook provides guidance for examiners to determine the *internal* cybersecurity risk of a company related to its own systems, but does not provide any guidance on analyzing the exposure to that company from writing Cyber policies. With a more detailed analysis of the policy provisions offered and the relationships managed by the carrier, regulators will have a clearer picture of the company's Cyber exposure and an opportunity to put appropriate safeguards in place.

The NAIC's Financial Condition Examiners Handbook and Troubled Company Handbook provide guidance to examiners and regulators. Those tools could be enhanced through the development of an analytical checklist for Cyber insurance. Example checklist questions include:

- Does the company have Cyber coverage in force? If so, what is the premium volume and amount of total exposure?
- Is the coverage sold as a stand-alone policy?
- Is the coverage sold as a rider or endorsement to another more traditional coverage? If so, which coverages are included in the underlying policy to which the rider is attached?
- What are all of the different benefits that are provided under the Cyber coverage? For example, are in-kind services provided for IT support, credit monitoring, data breach notification, and forensic analysis?

- What arrangements does the company have in place to provide in-kind services and other non-indemnity benefits under the Cyber coverage? For example, does the company have a panel of "breach coaches" who are familiar with the company's policies and the administration of benefits provided thereunder? Does the company have a Cyber claims "hotline" for claims reporting?
- Is coverage provided for government-imposed penalties, and if so, for which levels of government? For example, will state data breach penalties, Federal HIPAA penalties, or EU GDPR penalties be covered claims?
- What are the coverage triggers that are used in the Cyber policies? Are they "occurrence" or "claims made" policies? If the Cyber business is written on a "when discovered by management" basis, will a forensic report also be necessary to determine what management knew and at what time in order to trigger coverage?
- How many different Cyber policy forms, endorsements, or riders are in force?
- Are the Cyber benefits in actuality provided by a third party or fully reinsured?
- Is Excess Cyber coverage being provided?
- What are the range of limits provided under the various Cyber coverages?
- What are the largest limits provided on a single risk, across all layers?

Answers to the aforementioned questions will not only assist regulators, but also will give receivers and guaranty funds the tools to quickly determine company liabilities and be prepared to step in quickly and provide in-kind coverage to policyholders. Effectively administering these claims will require an increased level of coordination between regulators, receivers and the guaranty funds. It will also be interesting to reconcile the responses to these questions with the information contained on the Cybersecurity and Identity Theft Insurance Coverage Supplements filed by the troubled company.

Operational Readiness

Under more traditional property and casualty policies, it has been fairly straightforward to gain insight into the type and magnitude of the claims that a guaranty fund should expect by looking at the troubled company's annual statements. For the reasons expressed above, this will be difficult to carry out for Cyber writers unless some enhancements are made to the financial reporting of Cyber coverage by companies.

It will be helpful if financial regulators are able to share with receivers and guaranty funds on a confidential basis potential Cyber exposure in a troubled company facing liquidation. The "prevention and detection of insolvency" language found in most guaranty fund statutes may allow insurance departments to confidentially share certain information about a troubled company with a guaranty fund. In some cases, a standing confidentiality agreement for this purpose may be desirable. Early warning efforts from insurance departments will be important to receivers and guaranty funds so that they can prepare to appropriately protect policyholders and claimants under this line of coverage.

If a Cyber insurer falls into receivership or liquidation, receivers and guaranty funds will be required to provide the specialized services and benefits promised under those policies. As neither has a history of providing such services, receivers and guaranty funds will need additional lead time to analyze the Cyber contracts of the troubled company and establish contractual relationships with the same or similar vendors. It is important that guaranty funds and receivers become familiar with all aspects of handling Cyber claims, develop Cyber claims handling plans, and identify potential vendors and experts to provide the most common specialized services found as benefits in a Cyber policy.

It will be essential to the administration of a troubled Cyber insurance writer that regulators, receivers and guaranty funds collaborate early in the process to share relevant policy information, plan for retention or replacement of specialized vendors, and coordinate the handling of both existing and newly-reported claims.

Coverage and Priority Issues

Receivers and guaranty funds in each state should also consider likely points of stress when Cyber claims begin to interact with their statutes. In each state, they will need to consider coverage questions such as the proper application of claim caps and, given the compressed response timeline, an approach to "covered claim" determinations and dealing with non-covered claims. These are just a few of the issues that must be answered *before* the first challenging Cyber insolvency occurs.

Conclusion

The orderly resolution of a company that writes Cyber insurance will require tangible changes to the way our system collects and shares information. We recommend that the NAIC, IAIR and the NCIGF consider the following steps:

- Create a more transparent and easily accessible accounting of individual carriers' Cyber exposure that captures coverage across lines of business including endorsements;
- Develop a checklist and special interrogatories for financial examiners evaluating insurers that write Cyber policies;
- Amend the Receiver's Handbook to advise early engagement, including sharing of relevant confidential information, with the guaranty funds;
- Advise receivers and guaranty funds to establish a bank of vendors to ensure in-kind services are seamlessly provided on Cyber claims during an insolvency; and
- Ask guaranty funds to examine their statutes and establish plans for expediting "covered claim" determinations for certain newly-reported Cyber claims.

There is much to be done before the state resolution system is fully prepared for the smooth resolution of an insolvent Cyber insurance carrier, but now is the time to put in the work. With cooperation, we can address these challenges and guarantee protection for the policyholders in this growing and rapidly developing segment.

MEMORANDUM

TO: Innovation and Technology (EX) Task Force

FROM: Denise Matthews
Director, Data Coordination and Statistical Analysis

DATE: September 12, 2019

SUBJECT: Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement

The purpose of this report is to provide the Innovation and Technology (EX) Task Force with the information filed by insurers in the Cybersecurity Insurance and Identity Theft Coverage Supplement (Supplement) to the property/casualty (P/C) annual financial statement for 2018. The NAIC also receives data from Surplus Lines insurers, which is included in this report.

Overview

Cybersecurity continues to be crucial to effective and efficient operation of U.S. businesses. Cybersecurity breaches can cause a major drain on the U.S. economy. Insurers face cybersecurity risks in their daily operations, as do banks and securities firms. The financial services sector is susceptible to cyber threats for multifaceted reasons. Financial firms receive, maintain and store sensitive personal financial information for their customers. Insurers, in many cases, receive personal health information in addition to personal financial information. Insurers receive information from both policyholders and claimants.

Cybercriminals are interested in fraudulently obtaining and using sensitive information for financial gain. We know from observation of the dark web that personal health information continues to be more valuable than personal financial information. Nation states are also known to sponsor cyberattacks for espionage or to gain access to corporate trade secrets and business processes. Ransomware attacks are increasing and a continued area of concern because they are used to extort payments from compromised firms.

Insurers are selling cyber risk-management services and cybersecurity insurance products to businesses and individuals. It is to gain information and understanding about cybersecurity insurance markets that led regulators to design and implement the Supplement.

This year, insurers reported information based on the 2018 calendar year results. Based on the data filed, approximately 500 insurers have provided businesses and individuals with cybersecurity insurance, with 96%[1] of the insurers writing cybersecurity insurance as part of a package policy.

An overview shows a cybersecurity insurance market of roughly $2.03 billion in direct written premiums for insurers required to file the Supplement. This is a slight increase from last year's direct written premiums of $1.89 billion. Insurers writing stand-alone cybersecurity insurance products reported approximately $1.11 billion in direct written premiums, and those writing cybersecurity insurance as part of a package policy reported roughly $915 million in premium writings.

The remainder of this report will provide figures filed for each category and explain assumptions used to arrive at the $2.03 billion in direct written premiums by admitted insurers. This report will also discuss the entities' reporting data and assumptions related to entities where data on package policies is missing from the data set.

Cybersecurity Insurance Coverage

The Supplement requires insurers to report the following information on stand-alone cybersecurity insurance policies:

- Number of claims reported (first-party and third-party).
- Direct premiums written and earned.
- Direct losses paid and incurred.
- Adjusting and other expenses paid and incurred.
- Defense and cost containment expenses paid and incurred.
- Number of policies in-force (claims-made and occurrence).

[1] The number in NAIC's report from last year stated 47%; however, the number was actually 96%.

The Supplement requires insurers to report the following information on cybersecurity insurance coverage sold as part of a package policy:

- Number of claims reported (first-party and third-party).
- Direct premiums written and earned, if available or estimable.
- Direct losses paid and incurred.
- Adjusting and other expenses paid and incurred.
- Defense and cost containment expenses paid and incurred.
- Number of policies in-force (claims-made and occurrence).

Stand-Alone Policies

As noted in the 2018 report, the gap between earned and written premiums is indicative of a growing market. That gap has decreased between 2017 and 2018 indicating the market is maturing in the stand-alone cybersecurity insurance marketplace. Insurers writing this coverage reported $1.11 billion in direct written premiums spread among 46 groups of insurers (140 individual insurers). Direct earned premiums reported were $1.03 billion. The top 10 insurers wrote 82.3% of the total U.S. market, with the top 20 writing 94% of the market (Exhibit 1). The stand-alone cybersecurity insurance written premiums for 2018 increased by 12.02% since last year.

The loss ratios for stand-alone cybersecurity insurance range from zero to 106%. The loss ratios from the top 20 standalone insurers range from .03% to 82.7%. These loss ratios are listed in the chart below. It is important to note that the cybersecurity insurance market for cybersecurity insurance products is still nascent; therefore, an element of catastrophe exposure exists. A loss ratio of zero might be indicative of sound underwriting, but it might also simply indicate the selected businesses did not experience a cyber event in 2018.

Exhibit 1
Standalone Cyber Insurance Market Share by Individual Insurers
2018 Data Year

Rank	Company Code	Company Name	Direct Written Premium	Market Share	Loss Ratio (including defense and cost containment)	Cumulative Market Share
1	968	AXA INS GRP	255,874,528	23.0%	57.2%	23.0%
2	12	AMERICAN INTL GRP	232,312,591	20.9%	36.1%	43.8%
3	3548	TRAVELERS GRP	112,920,719	10.1%	27.7%	54.0%
4	37540	BEAZLEY INS CO INC	100,860,728	9.1%	6.1%	63.0%
5	212	ZURICH INS GRP	43,315,425	3.9%	18.2%	66.9%
6	23	BCS INS GRP	39,534,843	3.5%	13.5%	70.5%
7	158	FAIRFAX FIN GRP	38,145,472	3.4%	23.4%	73.9%
8	3098	TOKIO MARINE HOLDINGS INC GRP	34,858,640	3.1%	38.2%	77.0%
9	111	LIBERTY MUT GRP	33,427,580	3.0%	43.6%	80.0%
10	218	CNA INS GRP	25,032,362	2.2%	13.7%	82.3%
11	4698	ASPEN INS HOLDING GRP	21,073,367	1.9%	61.6%	84.2%
12	3416	AXIS CAPITAL GRP	19,592,044	1.8%	1.6%	85.9%
13	785	MARKEL CORP GRP	16,542,650	1.5%	60.2%	87.4%
14	4904	INTACT FINANCIAL GRP	13,439,331	1.2%	53.2%	88.6%
15	501	ALLEGHANY GRP	11,101,174	1.0%	12.1%	89.6%
16	4666	HISCOX INS GRP	10,595,387	1.0%	26.8%	90.6%
17	98	WR BERKLEY CORP GRP	10,176,206	0.9%	20.4%	91.5%
18	31	BERKSHIRE HATHAWAY GRP	10,069,160	0.9%	82.7%	92.4%
19	761	ALLIANZ INS GRP	9,743,451	0.9%	.03%	93.2%
20	783	RLI INS GRP	8,843,152	0.8%	4.9%	94.0%

Package Policies

The reported direct written premiums for cybersecurity package policies totaled $898.3 million. This year, only 9 out of 491, down from 16 out of 462 based on 2017 data, reported no premiums, generally indicating they were unable to break out the premium change for the cybersecurity coverage from the remainder of the package policy. To arrive at a figure representing a complete market, NAIC staff assumed the 9 insurers writing cybersecurity package policies where premiums were not reported would have reported premiums in the same ratio as those insurers reporting premiums.[2] The NAIC estimates $16.8 million of direct written premiums for those 9 companies. As a result, by extrapolation, the NAIC estimates the direct written premiums sold through package policies was approximately $915

[2] Nine of the 491 insurers reporting no premium represent 1.83% of direct written premiums for package policies.

million. This is an increase of a little more than 2%. The top 10 insurers writing package cyber insurance products represent 71.8% of the market, and the top 20 insurers represent 82.8% of the market. (See Exhibit 2.)

Exhibit 2
Package Cyber Insurance Market Share by Individual Insurers
2018 Data Year

Rank	Company Code	Company Name	Direct Written Premium	Market Share	Loss Ratio	Cumulative Market Share
1	626	CHUBB LTD GRP	320,729,113	35.7%	28.6%	35.7%
2	218	CNA INS GRP	58,324,863	6.5%	32.5%	42.2%
3	3416	AXIS CAPITAL GRP	56,408,989	6.3%	9.1%	48.5%
4	91	HARTFORD FIRE & CAS GRP	39,704,460	4.4%	16.4%	52.9%
5	3219	SOMPO GRP	34,054,366	3.8%	56.7%	56.7%
6	3548	TRAVELERS GRP	33,309,900	3.7%	4.5%	60.4%
7	111	LIBERTY MUT GRP	33,067,460	3.7%	34.1%	64.1%
8	23	BCS INS GRP	29,969,858	3.3%	6.3%	67.4%
9	457	ARGO GRP US INC GRP	20,593,376	2.3%	27.4%	69.7%
10	31	BERKSHIRE HATHAWAY GRP	18,564,643	2.1%	68.9%	71.8%
11	244	CINCINNATI FIN GRP	16,785,618	1.9%	7.0%	73.6%
12	88	THE HANOVER INS GRP	12,761,012	1.4%	9.1%	75.1%
13	69	FARMERS INS GRP	12,640,773	1.4%	3.6%	76.5%
14	37540	BEAZLEY INS CO INC	10,087,075	1.1%	24.4%	77.6%
15	3098	TOKIO MARINE HOLDINGS INC GRP	9,733,560	1.1%	3.4%	78.7%
16	98	WR BERKLEY CORP GRP	9,283,630	1.0%	0.3%	79.7%
17	7	FEDERATED MUT GRP	8,879,172	1.0%	2.5%	80.7%
18	140	NATIONWIDE CORP GRP	7,237,205	0.8%	15.1%	81.5%
19	785	MARKEL CORP GRP	5,970,595	0.7%	0%	82.2%
20	4790	MMIC GRP	5,804,655	0.6%	14.6%	82.8%

Total Admitted Market

Thus, $2.03 billion is the reported and estimated total of direct written premiums for cybersecurity insurance coverage on a stand-alone and package policy basis for 2018 by insurers obligated to complete and submit NAIC statutory financial statements. This is a 6.81% increase from last year's direct written premium.

In order to provide perspective and context, it should be noted that $2.03 billion in direct written premiums is a small percentage of the $621 billion[3] in net written premiums reported by P/C insurers for 2018. All of these writings are supported by $780 billion[4] in policyholder surplus held by insurers.

Surplus Lines Insurers

The reported information for admitted insurers is limited to only those insurers required to file a P/C annual financial statement with the NAIC. To evaluate this limitation, one must understand the types of insurers writing P/C business in the U.S. and whether each type is required to report information to state insurance regulators. This may be well understood, but it is important for readers not completely familiar with the U.S. regulatory framework to understand, from a state insurance regulator's perspective, the admitted and surplus lines markets.

Generally, the U.S. regulatory system for P/C insurance views insurers as belonging in one of three classifications: 1) domestic; 2) foreign; or 3) alien. A domestic insurer is one licensed or admitted in a state it selects to be its home state. A foreign insurer is one licensed or admitted in a state that is domiciled in another state. An alien insurer is one domiciled in another country. Generally, the states insist insurers be licensed or admitted in the state as a prerequisite for selling P/C insurance products. However, state legislatures recognize not every person or business seeking coverage for unique risks can find it from a licensed or admitted insurer. Thus, state legislatures have allowed non-licensed insurers to write P/C business under certain circumstances.

The insurers doing business as non-licensed or non-admitted insurers are known as surplus lines insurers. They serve as an alternative marketplace to provide coverage for unique exposures and often serve as a testing ground for product innovations before they become mainstream. Offering coverage on a surplus lines basis allows the insurer greater freedom in pricing and does not require formal prior approval of contract language.

This is the third year the NAIC received information filed by surplus lines insurers. Surplus lines data received indicate premiums of $1.2 billion in cybersecurity stand-alone package policies in 2018, which is a 36.3% increase since last year. The surplus lines premium

[3] *http://naic.org/documents/topic_insurance_industry_snapshots_2018_ye.pdf.*
[4] Ibid.

for cybersecurity package policies for 2018 is $368.13 million. This is a decrease of 17.2% from last year's numbers. The total written premium for both types of policies is $1.57 billion, indicating a total increase of 23.7%.

The Overall Cybersecurity Insurance Market

For 2018, the total cybersecurity insurance market in the U.S. was approximately $3.6 billion, which is a 14.54% increase from last year. This figure includes the stand-alone and package cybersecurity insurance premiums reported in the NAIC statutory financial statements, an estimate of the missing package cybersecurity premiums where insurers were unable to separate cybersecurity premiums from the package premium, and the information reported by surplus lines insurers.

The vast majority of third-party coverage for standalone cybersecurity policies continue to be written on a claims-made basis. From a solvency risk-management perspective for insurers, the claims-made contract generally serves to limit exposure to the insurer compared to an occurrence policy by placing time limits on when the insured event must be reported to the insurer. While this is good for insurers, it is a coverage limitation from a policyholder perspective.

Identity Theft Coverage

From a market perspective, the year-end 2018 data continues to indicate that U.S. insurers' most common product related to cybersecurity is in the form of identity theft coverage, where insurers wrote approximately 20.7 million policies including identity theft coverage as part of a package policy. This compares to only 236,925 policies that were stand-alone identity theft coverage.

The year-end 2018 data for identify theft coverage indicates the stand-alone premium on the 236,925 policies was $9.3 million, or approximately $39.35 per policy. The year-end data for identity theft coverage shows reported package policy premiums of $216.6 million and 20.7 million policies sold, which is approximately $10.45 per policy. It is important to note the cost of purchasing this coverage varies from insurer to insurer depending on other coverages purchased with the homeowner's policy or another package policy. Additionally, due to recent data breaches, many people are receiving identity theft coverage as a result of the breach. It is also important to keep in mind that oftentimes another policy may include this coverage for no charge; therefore, the cost per policy may be slightly higher or lower.

Conclusion

This report summarizes some interesting findings. The data and estimates based on the data indicate the total U.S. market for cyber insurance is roughly $3.6 billion. Having a time series will allow state insurance regulators to track market growth and pinpoint areas where further regulatory oversight may be needed. The data indicate the cyber insurance market slowed between 2017 and 2018.

It is important to mention that reinsurance is not reflected in the data. An estimate by Aon indicates that $800 million in cyber reinsurance was placed in 2018. AM Best postulates that treaty reinsurance is more widely available than facultative reinsurance. AM Best also said that most treaties are being written as quota share reinsurance treaties. It is noteworthy to mention that most of the quota share treaty agreements include a loss ratio cap. A systemic event continues to be the top threat to cyber insurers' solvency.[5]

The chart below depicts information collected from all four years of data collection.

Year	Direct Written Premium Stand-alone Cyber Policies	Direct Written Premium Package Cyber Policies	Direct Written Premium Stand-alone Surplus Lines Cyber Policies	Direct Written Premium Package Surplus Lines Cyber Policies	Stand-alone Policy Totals (Admitted and Surplus Lines)	Package Policy Totals (Admitted and Surplus Lines)	Total Cyber Premiums Written
2015	$ 483,197,973	$ 932,645,734	Not Reported	Not Reported	$ 483,197,973	$ 932,645,734	$ 1,415,843,707
2016	$ 811,057,406	$ 863,769,169	$ 552,226,000	$ 156,285,000	$ 1,363,283,406	$ 1,020,054,169	$ 2,383,337,575
2017	$ 994,259,551	$ 896,424,050	$ 765,129,000	$ 431,423,000	$ 1,759,388,551	$ 1,327,847,050	$ 3,087,235,601
2018	$1,113,865,104	$915,046,459	$1,200,880,000	$368,134,000	$ 2,314,745,104	$ 1,283,180,459	$ 3,597,925,563

The 2018 data indicates cyber insurance continues to be an evolving market. According to a recent survey conducted by the Council of Insurance Agents and Brokers (CIAB), the take-up rate for cyber insurance remains relatively low at 33%, while capacity appears to be plentiful or is increasing. Their report also stated that $2.8 million is the typical cyber insurance policy limit.[6]

Caveats

In the 2015 report, surplus lines premium information was not included; however, this data was collected for the 2016, 2017 and 2018 data years.

[5] AM Best's Market Segment Report, June 17, 2019.
[6] Ciab.com/resources/cyber-insurance-by-the-numbers

What Others are Saying About the Cybersecurity Insurance Markets

"Most companies writing cyber insurance are remaining prudent about their total exposure, and cyber exposure relative to policyholder surplus is limited." *AM Best*.

"Pricing will remain stable, and capacity will keep up with demand" and "Carriers will begin to address whether cyber is a product or a peril."—*Willis Towers Watson*

"Cloud insecurity grew in 2018, and unfortunately, it will carry on growing even more in 2019. Increasing amounts of data are being deployed from disparate parts of organizations, with more and more of that data ending up unsecured. Despite the continual publicity around repeated breaches, the majority of organizations do not have good housekeeping deployed and enforced across their whole data estate in the cloud."—*Digital Insurance*

"Cyber risk is now widely accepted as being one of the top emerging risks."—*JLT Specialty*

In 2018, the greatest challenge organizations will face is simply keeping up with and staying informed about the evolving cyber risk landscape. The threats that can impact organizations vary widely by industry, size, and regions. It is incumbent upon organizations to understand the risks they face and to address them on a proactive basis."—*Aon*

W:\National Meetings\2019\Fall\TF\Innovation\Cybersecurity_Supplement_Report\Cyber_Supplement_2019_Report_Final.docx