TO: Cybersecurity (EX) Task Force

FROM: Eric Nordman, CPCU, CIE, MCM
Director, Regulatory Services Division & the CIPR

Dan Daveline,
Director, Financial Regulatory Services Division

DATE: August 27, 2016

SUBJECT: Report on the Cybersecurity Insurance Coverage Supplement

The purpose of this report is to inform the Cybersecurity (EX) Task Force about the information filed by insurers in the Cybersecurity Insurance and Identity Theft Coverage Supplement (the Supplement) to the Property and Casualty Annual Statement for 2015. The report will also address some shortcomings in the data collection process and make some suggestions for future actions for the Task Force to consider.

Overview

Cybersecurity is 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 perhaps the most under attack from cyber criminals. The reason for the attacks is multifaceted. Financial firms receive, maintain and store sensitive personal financial information from their customers. Insurers, in many cases, receive personal health information in addition to personal financial information. For insurers, information may be provided by policyholders or claimants. Cyber criminals are interested in this sensitive information as it can be used for financial gain by stealing a person's identity for fraudulent purposes. We know from observation of the dark web that personal health information is much more valuable these days than personal financial information. Nation states are also known to sponsor cyber-attacks for espionage or gaining access to corporate trade secrets and business processes.

© 2016 National Association of Insurance Commissioners

Insurers are selling cyber risk management services and cybersecurity insurance products to businesses and individuals. It is to gain information and understanding about the cybersecurity insurance markets that led regulators to design and implement the Supplement. The first year the Supplement was required to be filed was with the 2015 Annual Statement filed in April of 2016. The data filed provides some interesting results. The initial results of these filings indicate over 500 insurers have provided businesses and individuals with cybersecurity insurance, with the vast majority of these coverages written as endorsements to commercial and personal policies. An overview shows a market of roughly $1.5 billion in direct written premium for insurers required to file the Supplement. Insurers writing standalone cybersecurity insurance products reported approximately $500 million in direct written premium and those writing cybersecurity insurance as part of a package policy reported roughly $ 1.0 billion in premium writings. The remainder of the report will provide figures filed for each category and explain assumptions used to arrive at the $ 1.5 billion in direct written premium. It will also discuss the entities reporting data and which entities might be missing from the data set. The report concludes with some recommendations for the Task Force to consider going forward.

Cybersecurity Insurance Coverage

The Supplement requires insurers to report the following information on standalone cybersecurity insurance policies:

- Number of claims reported (First Party & 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)

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 & 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)

© 2016 National Association of Insurance Commissioners

Standalone Cybersecurity Insurance Policies

Perhaps the most interesting information is the size of the standalone cybersecurity insurance marketplace. Insurers writing this coverage reported $483,197,973 in direct written premium spread among 48 insurer groups (116 individual insurers). Direct earned premium reported was $373,742,189. Having less earned premium than written premium is indicative of a growing market. The top ten insurers wrote 78.7% of total U.S. market with the top 20 writing 95.8% of the market.

Loss ratios for standalone cybersecurity insurance were all over the map ranging from zero to over 500%. This too was not overly surprising. The market for cybersecurity insurance products is a new one and it is one with an element of catastrophe exposure. A zero loss ratio might be indicative of sound underwriting, but it might also simply be luck in selecting businesses that did not get hacked in 2015. The over 500% loss ratio occurred in an insurer group with less than $400,000 in direct written premium. Again, it could be indicative of poor underwriting or simply bad luck to insure a policyholder having a breach in 2015.

To keep things in perspective, the reader should remember $1.5 billion in direct written premium is only a very small percentage of the $522.4 billion in net written premium reported by the property and casualty insurers for 2015. All of these writings are supported by $703.6 billion in policyholder surplus held by insurers.

Package Policies

The reported direct written premium for cybersecurity package policies totaled $515,100,239. However, 257 insurers of the 574 insurers reported no premiums, generally because they could not 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 257 insurers writing cybersecurity package policies where premiums were not reported would have reported premiums in the same ratio as those insurers reporting actual premiums.

The actual mathematical calculation to extrapolate the premium dollars not reported under package policies follows:

- 257 insurers of 574 insurers reported no premium, representing 44.77% of the insurer population.
- The inverse of 44.77% is 55.23%.
- Then divide the actual package premium of $515,100,239 by 55.23% to get $932,645,734.
- As a result, by extrapolation we estimate approximately $933 million was the direct written premium sold through package policies.

© 2016 National Association of Insurance Commissioners

Thus, we wish to inform you $1,415,843,707 is the reported and estimated total direct written premium for cybersecurity insurance coverage on a standalone and package policy basis for 2015.

Another interesting observation about the cybersecurity insurance policies sold on a standalone basis is most of the third party coverage is written on a claims-made basis. Approximately 82% of the policies were claims-made. 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 2015 data clearly indicates that U.S. insurers' most common form of risk related to cybersecurity is in the form of identity theft coverage, where insurers wrote approximately 16.6 million policies including identity theft coverage as part of a package policy. This compares to only 496,000 policies that were stand-alone identity theft coverage.

From a risk perspective, the year-end 2015 data for identify theft coverage indicates the stand-alone premium on the 496,000 policies was $21.2 million, or approximately $42 per policy. Based upon this average of $42 per policy, the total amount of estimated annual premium on the 16.6 million policies with identify-theft as part of a package policy is still only approximately $700 million.

Caveats

When one uses data to gain information, it is important to understand its source, its attributes and its limitations. There are some important limitations for readers of this report to consider. The first limitation is the reported information is limited to only those insurers required to file a Property and Casualty Annual Statement with the NAIC. To evaluate this limitation, one must understand the types of insurers writing property and casualty business in the U.S. and whether each type is required to report information to U.S. regulators. With apologies to regulators who already understand what is said in this section, we believe it is important for readers not completely familiar with the U.S. regulatory framework to understand, from a state insurance regulators' perspective, the admitted and surplus lines markets.

The U.S. regulatory system for property and casualty insurance views insurers as belonging in one of three classifications. They are: domestic, foreign and alien. A domestic insurer is one

© 2016 National Association of Insurance Commissioners

licensed or admitted in a state it selects to be its home state. A foreign insurer would be one licensed or admitted in a state that is domiciled in another state. An alien insurer is one domiciled in another country. Generally states insist insurers be licensed or admitted in the state as a prerequisite for selling property and casualty 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 property and casualty 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. Such is the case for cybersecurity insurance products. Offering coverage on a surplus lines basis allows the insurer greater freedom in pricing and does not require formal prior approval of contract language.

If an insurer is licensed or admitted in one or more states, it is required to submit an Annual Financial Statement, including the Supplement. Thus, all domestic and foreign insurers are required to file the Supplement as they will be considered an admitted insurer in at least one state. Alien insurers can choose to be licensed or admitted in one or more states if they wish. If they do choose to be licensed or admitted, then they too must file the Supplement. However, if an alien insurer decides not to become licensed in any state, the District of Columbia or U.S. territory, then no Supplement filing is required. The premium writings by alien surplus lines insurers are missing from the information contained in this report. Since we believe there may be a significant amount of premium written by alien surplus lines insurers, the reader should be cognizant of this potentially important missing element.

What Others are Saying about the Cybersecurity Insurance Markets

"Cyber coverage is the fastest growing surplus lines business in history and it was caused by a regulation, not by some other market factor. It's a $1 billion line right now."—Benjamin J. McKay, Executive Director of the Surplus Line Association of California

"The cyber insurance marketplace has grown to over $2 billion in gross written premiums with industry prognosticators forecasting it to double by 2020. The number of carriers offering cyber insurance has increased following a spate of cyberattacks that have brought the potential and need for such insurance into sharper focus."—PartnerRe

"We expect worldwide spending on Cybersecurity products and services to eclipse $1 trillion for the five-year period from 2017 to 2021"—Steve Morgan, Founder and Editor-In-Chief at Cybersecurity Ventures

© 2016 National Association of Insurance Commissioners

"Cyber insurance is a potentially huge, but still largely untapped, opportunity for insurers and reinsurers. We estimate that annual gross written premiums are set to increase from around $2.5 billion today to reach $7.5 billion by the end of the decade."—PwC Report—Insurance 2020 & beyond: Reaping the dividends of cyber resilience

"Annual premium volume information about the U.S. cyber-risk market is hard to come by, but in reviewing the market, we have concluded that the annual gross written premium may be as much as $3.25 billion (up from $2.75 billion in last year's report)."— Richard S. Betterley, CMC, President, Betterley Risk Consultants, Inc. from Cyber/Privacy Insurance Market Survey—2016

"The cyber market is growing by double-digit figures year-on-year, and could reach $20 billion or more in the next 10 years. …fewer than 10% of companies are thought to purchase cyber insurance today."—Nigel Pearson, Global Head of Fidelity, Allianz Global Corporate & Specialty

Recommendations for the Task Force

A major caveat contained in this report is the missing information on the amount of premium written by alien surplus lines insurers. Staff believes there may be significant premium writings, particularly for standalone cybersecurity insurance policies, in this segment of the overall markets. Staff recommends the Task Force consider approaching the Surplus Lines (C) Task Force to request making submission of some or all of the information contained in the Supplement a condition for continuing to be listed on the *Quarterly Listing of Alien Insurers*.

A second staff recommendation is for the Task Force to take comments from interested parties on how the instructions or the format of the Supplement could be improved.

Conclusion

While the first report of any data collection exercise is challenging, the quality of the data improves with subsequent filings. This report summarizes some interesting findings. If information can be obtained from the alien surplus lines insurers, a more complete picture of the 56 U.S. cybersecurity insurance markets will emerge. Having a time series will allow regulators to track market growth and pinpoint areas where further regulatory oversight is needed.

© 2016 National Association of Insurance Commissioners