National Insurance
Alliance Limited

19th April 2019

Cyber Insurance Predictions: Strong Drivers for Growth Ahead

Cyber insurance is trending upward, the industry is growing, and the technology around it is evolving at a very quick pace. While predictions are always hard to make, here are trends that are likely to catapult the cyber insurance industry forward, creating fertile ground for growth in 2019.

Regulation

When it comes to regulation and cyber insurance, we need to think of indirect and direct regulations that may affect the market. Additionally, we need to consider how regulation affects insurers and insureds both from an affirmative and silent risk perspective. Silent cyber risk refers to potential cyber-related losses due to inadvertent coverage within other P/C insurance policy wording which excludes cyber risk. Just look at the rapid increase in data privacy laws, such as those for personally identifiable information (PII) in the U.S., the HIPAA Privacy Rule (covering medical records and personal health information in the U.S.), the Payment Card Industry Data Security Standard (PCI DSS), which is a global standard, and the EU's General Data Protection Regulation (GDPR) – to name a few.

One of the ways businesses deal with risk hedging for these laws is via cyber insurance. While they actively try to focus on reducing the chances that leaks of this type of data may occur, they ultimately know that in the cyber landscape, anything can happen and thus insurance is key for their risk management strategy.

Additionally, there is direct regulation that specifically targets cyber insurers. For example, the EU's largest insurers are to be assessed for their exposure to, and the way in which they deal with cyber risks in any insurance book they own. Most recently, on Nov. 10, the European Insurance and Occupational Pensions Authority (EIOPA), together with the National Association of Insurance Commissioners (NAIC) and the Federal Insurance Office (FIO) of the U.S. Department of Treasury hosted the sixth EU-U.S. Forum in Luxembourg and discussed challenges and opportunities related to cyber risks, the use of big data, artificial intelligence and intra-group transactions in multinational insurance groups. It is fair to predict that EIOPA's stress test for insurers may be something that U.S. regulators may be looking to implement as well.

Development of Cyber Insurance-Linked Securities (ILS) Market and Cyber Risk Pools

Insurance professionals are looking for innovative ways to expand the availability of cyber insurance and creative ways to enter the market. Cyber pools can potentially offer a facility for providing cyber insurance to corporate buyers and the use of capital markets funding, to back the risk, can allow for larger policy limits for specific use-cases. It can also be a safer way for professionals to learn the cyber risk landscape and become a part of the market.

While property catastrophe risks are the prominent line of business across the ILS sector, both investors and sponsors are increasingly looking at other emerging risks, such as cyber, according to Willis Tower Watson's ILS survey report, published in October 2018, indeed, the Singaporean government announced in October 2018 that it plans to launch the world's first commercial cyber risk pool. This facility will provide cyber insurance to corporate buyers in the Asia region and will be backed by insurance-linked securities and reinsurance. It is a great foreshadowing of similar moves soon expected in the European and American markets.

For these initiatives to develop, they'll need to work with vendors that can provide advanced cyber threats intelligence, risk modelling, and rating services to properly assess cyber risk within a diverse set of policies. As these vendors better predict cyber catastrophes that may affect policies, their track records will increase insurers' confidence in these products and thus reinforce the growth of the cyber insurance market.

Awareness Around Silent Cyber Risk

Awareness about silent cyber; also referred to as non-affirmative cyber will increase. Insurers are gradually realizing they have unquantified exposures and are looking for solutions to quantify their exposures as well as give them the option to amend or exclude coverages in other lines that may leave them overly exposed. For example, we are still seeing the effects of the NotPetya ransomware attack in 2017 on Maersk, FedEx, and other companies. The insurance industry loss from this attack has been estimated by RMS at up to $3 billion.

Of course, regulations set by EIOPA (as discussed above), will also help promote this trend of quantifying cyber risk, while rating agencies are likely to demand that insurers quantify their silent exposure. For example, in November, Moody's announced it will soon start using its credit-rating expertise to evaluate organizations on their risk of a major impact from a cyber-attack. As awareness around non-affirmative cyber grows, insurers will be making larger strides to make changes to overcome coverage ambiguity.

Growth of Cyber MGAs/MGUs Across the Globe

Reinsurers currently seek specialized entities to distribute specific lines of products. The increase in cyber-focused MGAs is most likely due to the need for deep expertise on the risks faced with providing cyber insurance and the need for dedicated efforts to best address the needs of cyber insurance purchasers. The trends in the growth of MGAs and MGUs are being driven by both traditional and new companies. For example, Aon recently launched a new unit, Carrier Solutions, to grow its MGA and MGU network. Further, insurtech MGAs, such as Coalition, At Bay and Zeugro, has seen success. The combination of these two types of efforts will spearhead the MGA/MGU industry as traditional insurers vie for ways to grow their business and insurtech find new creative ways to competitively enter the market with technological advancements. Specialized cyber MGAs will be a significant part of the future and start to form worldwide.