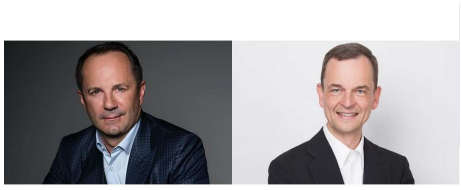
The industry is starting to understand an infant cyber market: Guenther, Hacker

21st November 2019 - Author: Luke Gallin (https://www.reinsurancene.ws/about/#team)

Still in its infancy, the global cyber risk market continues to grapple with data and modelling challenges, but increasingly, re/insurers are becoming aware of a need for new and innovative approaches.

This is according to the owner and founder of PeriStrat GmbH, Hans-Joachim Guenther and Peter Hacker, a globally recognized cyber security expert and advisor to organisations, regulators and corporate boards. In a recent interview with Reinsurance News, the pair discussed the current embryonic state of the cyber risk modelling market, viewed as one of the biggest challenges and opportunities for global insurers and reinsurers.



Hacker (left), Guenther (Right)

Guenther and Hacker underlined a significant cyber risk protection gap, estimating a coverage level, for both affirmative and non-affirmative combined, of between 17% and 22% of actual economic losses.

With as much as 83% of exposures not being covered by protection, Reinsurance News questioned the pair on whether insurers and reinsurers are doing enough to meet the challenges.

“The demand for insurance outside the US isn’t yet matured because many potentially insured do not comprehend the risk they are exposed to. Moreover, insures won’t have enough access to corporate boards and even if they have, they struggle to explain their value proposition to Boards.

“The (re)insurance industry is not yet able to serve the potential demand because of multiple uncertainties around risk management of a highly dynamic and contagious exposure.

“Without any doubt, the real cyber loss exposure is significantly underinsured at this stage, thus insured losses will be much smaller than economic losses,” said Guenther.

Discussing demand for protection, and Guenther said that given the shift from tangible into intangible asset values, demand for affirmative cyber cover will grow exponentially. Furthermore, increased awareness of the risks and a greater understanding is also likely to drive greater demand.

Both Guenther and Hacker described the cyber insurance market (outside the US) as “infant”, highlighting that the direct insurance sector began to respond to perceived market demand for protection before fully understanding what might be already covered in the underlying P&C sector.

“But (re)insurance isn’t driving or yet innovating this space and we expect a lot of additional product development will follow claims experience as it did historically. However, this is in our view a dangerous path because of the virulent nature of cyber exposure. As an example: frequency of extortion cases. It is an affirmative coverage element, we feel should be entirely separate and on a stand-alone policy basis be handled like in K&R,” explained Hacker.

Cyber is an inherently and extremely complex exposure and one of the key challenges for re/insurers when trying to adequately understand the risk and potential financial impact, is a lack of historical data.

Hacker agreed that the modelling itself is “a major challenge,” but explained that while historical data will be important to verify certain modelling results, it will never be as important as it was in the natural catastrophe space. What really counts is active threat intelligence (‘insight-out’), rather than passive threat intelligence (‘outside-in’) or proxy and secondary data.

“The reason is simple: cyber exposure isn’t the result of acts of god but its man-made driven by criminal intent and with limited diversification levels compared to nat-cat. Threat actors are constantly changing and number of threat vectors behind attacks are rapidly developing which creates a complex and evolving risk landscape per industry or economy” said Hacker.

Guenther added, “Useful data is scarce, incident data isn’t comparable with actuarial loss frequencies, the dualism between silent and affirmative cyber require different severity views etc. The art of Cyber Risk Models lags 20 years behind Natural Catastrophe Assessment Models in Reinsurance and many current modelling approaches require single risk information but cannot handle aggregate portfolio situations.”

According to Guenther and Hacker, another major challenge will be the transition from silent, or non-affirmative to only affirmative protection.

“This will require a major contract wording clean-up which will get interference from competition as a natural business behaviour will try to make sure not to lose any market share thus there will be natural reluctance to be a first mover,” said Guenther.

Regarding silent cyber, Hacker continued to explain that the industry is starting to understand the potential dimension of silent cyber exposure.

“Apart from the size dimension both insurance demand and insurance supply recognize that silent cyber comes along with significant contract uncertainty. Pending court cases underscore this aspect. We are convinced this aspect will become a push factor to eliminate silent and covert this in affirmative, properly defined cover. Ambiguous wordings do not allow creating a sustainable value proposition.

> “There is simply too much uncertainty around triggers (Cyber Act, Cyber Incident), cyber event definitions (if any), write-backs (physical versus non-physical damages), non-kinetic war implications (e.g. cyber warfare vs hostile act) or simply whether data would represent physical assets. No party can sustain such contract uncertainty,” he said.
>
> “The industry also understands that cyber will require new and well-designed risk management approaches to cope with the contagious nature of this exposure. The push gets amplified through questionnaires and pressure from regulators, policy makers and rating agencies and finally boards who must look into this as part of their fiduciary duties,” added Guenther.
>
> Alongside silent cyber and the challenges here, a further concern for Guenther and Hacker is around state-sponsored cyber-attacks and the pair questioned whether governments should provide a state sponsored pool for such an event, similar to the French natural disaster compensation scheme.
>
> “In a nutshell to address these challenges, you have to combine detailed skills in both cyber security understanding, profound access to verified/transparent/ring-fenced active threat intelligence data, in particular in-depth (re)insurance knowledge and capabilities (wordings, pricing and actuarial) and incident management. Experience suggests that reinsurers should focus on developing their own treaty aggregation model.
>
> “Whilst this is a significant investment (6-9 months), they will have something bespoke built around their actual portfolio (qualitative and quantitative aspects) and fitting in their proprietary risk management frameworks by themselves.
>
> “Incident Data is the oil for the engine, but aggregation capabilities across the entire value chain are the real engine,” said Guenther and Hacker.