CYBER RISKS – THE KNOWN UNKNOWN EMERGING EXPOSURE

In this interview **Hans-Joachim Guenther** and **Peter Hacker** give an update on progress of the cyber pool announced at SIRC 2018 – and how industry thinking around cyber is developing.

Mr Hans-Joachim Guenther, reinsurance expert and risk thought leader.

Mr Peter Hacker, cyber security expert and risk thought leader.

What makes cyber risks unique? The industry is used to handling catastrophe losses in excess of $100bn.

HJG: First, cyber attacks are global. Thus, writing a global portfolio of cyber risks does not provide the diversification benefit like in natural catastrophes business. Second, cyber-attacks are manmade, driven by criminal motivation to steal knowledge, intellectual property and money or destroy and disrupt. State-sponsored attacks are worse in one aspect as they seek to infiltrate or damage entire economies. State-sponsored attacks go after materially important companies, critical infrastructure including health care and utilities, seek contagious effects creating a chain reaction through a high number of damaged entities with the intend to destabilise a country. Cyber risk is highly contagious.

PH: Most important, the intention of such threat actors is either to distract from the main targets and/or wipe networks, systems or data they infect. Such attacks will have impact across industries and not just one.

At SIRC 2018 an announcement was made about setting up a cyber pool with capacity of up to $1bn. What's happened since then?

PH: In the months following the announcement, it became clear that the industry wouldn't be prepared to share capacity in a pool structure but strongly believes in its own ways to serve the markets. However, there is a common interest to understand fully the underlying threats and the way an incident will transform into economic and (re)insurance loss patterns. In other words, there is strong consensus amongst a range of market players that the industry needs to take a fast-forward learning approach to stay ahead of a rapidly emerging risk.

Do you say the pool failed?

PH: No. The initiative became focused on what the market ultimately is looking for and I am proud to be at the helm of this initiative. Encouraged by our local as well as global (re) insurance partners, as a first stage, we undertook an in-depth, ground-up loss cost analysis based on a specifically defined, global risk portfolio and scenarios. The scenarios are based on massive power outage or major cloud operation and domain name servers failure resulting from a coordinated global cyber-attack, using the combination of a high volume and intensity driven distributed denial-of-service attack with two to four attacking vectors, one of them a major ransomware backing a wiper. The worst scenario is built upon a combination of both.

What is the role of SRA? Didn't they front-run the initiative?

PH: SRA was the incubator for the initiative's launch at SIRC 2018. SRA clearly honoured its independent role as a representative of the Singapore reinsurance market and stayed hands-off in any of the bilateral work between me and the subscribing (re)insurance partners.

Is there any tangible achievement so far?

PH: Yes. Meanwhile, the results and recommendations have been presented in Singapore and internationally amongst the partners. In a next step, we are discussing with the reinsurance industry and the Monetary Authority of Singapore to set-up a cyber education academy and an alternative risk transfer mechanism that would allow governments to manage the currently existing insurance gap.

Cyber risks will impact all industries, many economies and the (re)insurance industry. The contagious element of cyber requires close cooperation and working relationships between corporations, (re)insurance and capital markets as well as regulators and policy makers. No party is influential enough to resolve the unparalleled risk challenges on its own.

What concrete findings did you encounter following your scenario approach?

PH: We looked at two scenarios and a combination of the two. We predict global economic damages at the levels of $121bn, $185bn and $234bn and insurance losses at $27bn, $33bn and $40bn for the respective failures. The total amount of insurance claims would divide among 16%-20% for 'silent' components (property damage, business interruption (BI), marine and liability) to approximately 80%-84% for affirmative coverage elements (e.g. privacy liability, network security liability, network or security failure, cyber extortion, data asset protection cost, contingent BI liabilities and incident response cost). This spread assumes that state-sponsored attacks fall within the hostile act exclusion, data would not represent physical asset and D&O claims remain minor. The outcome of pending court cases might therefore well influence the silent cyber losses and our model in future.

What is the loss spread across industries? Are there any specific differences across continents?

PH: In our scenario portfolio we would forecast incident notifications rates from 11%, 18% to 24%, i.e. x% of all risk included in the scenario will record an incident, and with actual combined damage ratios ranging from 6%, 10% to 14%, i.e. x% of all risks which recorded an incident will suffer an economic loss.

The losses (consolidated at HQ for geographical tracking) would occur in North America (48%-60%), Europe (18%-23%), Asia (15%-17%) and ROW (7%-12%), and mostly in sectors such as finance, critical infrastructure, healthcare, manufacturing and retail. The 'hit ratios' per industry very much differentiate across the continents. For instance, in Asia, depending on the respective economy, healthcare often ranks first followed by critical infrastructure and/or finance, hospitality, retail, manufacturing and services. The reasons are various, but ultimately linked to the IT infrastructure used, investment into network security and exposure to state-sponsored cyber attacks.

Does insurance satisfy the demand for coverage?

HJG: You are asking two questions in one. In my view the demand for insurance isn't yet matured because many potentially insureds do not comprehend the risk they are exposed to. And 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.

Contagiousness is not really a new challenge for the industry?

HJG: There are major differences that need to be understood. It's the way this exposure finds its way into (re)insurance. Next to an immature market stage of affirmative cyber covers existing policies cover elements of cyber losses on a non-affirmative ('silent') basis.

PH: When looking at cyber coverage definitions is certainly not that straightforward. Can you really define a dynamically evolving risk like cyber accurately and consistently in words or rely on any case law on the interpretation of cyber (re)insurance contracts? What about the interpretation war or hostile act

exclusions? Should non-kinetic war e.g. from cyber-attacks also be excluded by the hostile act? Should exclusions be tight on silent but more relaxed for affirmative cyber covers where premiums get charged explicit? Even more, are current exclusions in non-affirmative policies fit for purpose at all? Are new clauses closing any wordings gaps?

What does this mean?

HJG: Policy wordings, and in particular property, engineering, marine, cargo and all risk wordings, have been widened to include miscellaneous additional losses as a result of price competition. Wordings softened and tend no longer to distinguish between data that is regarded as a tangible or intangible asset or whether business interruption (BI) or contingent BI losses require physical damage to assets or just disruption of any asset in the value chain. As a result, many wordings eventually assume losses from cyber attacks even though the contractual parties may never have intended those loss scenarios to be part of the insurance coverage. (Re) insurance never considered the premiums that should be charged for these silent cyber exposures. The ambiguity of wordings has already led to court cases with insureds seeking court orders to be reimbursed under property policies.

So cyber risks are uninsurable?

HJG: I think this is too easy. Historically the insurance industry has significantly advanced into areas which were once recognised as uninsurable. Just look at the early stages business interruption covers, contingent BI or environmental impairment covers. All this growth in risk capacity was built upon vision, careful risk management and multi-disciplinary knowledge pooling. But it was also responding to demand for insurance from parties who could not afford to keep these loss potentials on their own balance sheets.

What are the fundamental modelling challenges?

PH: Natural catastrophes are based on acts of god whereas cyber exposures will require more complex methodologies and cannot be built on experience due to its man-made criminal dynamic. So far cyber risk model vendors target predominantly direct insurance based on a single risks (insured) assessment. Therefore, their models are barely fit for purpose for aggregate portfolio assessments like reinsurance. Nat CAT models were improved over decades to their current levels of accuracy. Today, cyber risk models lag 20 years behind Nat CAT assessment models. Generally accepted data standards in Nat CAT like CRESTA zones or long-standing experience of how incidents transform into damages are missing in cyber. Cyber exposures and the relevance of contract wording language requires the development of bespoke modelling approaches which combine qualitative with quantitative aspects. For the Singapore cyber initiative, we developed our own bespoke cyber approach enriched by in-depth understanding of contractual (re) insurance language.

Do you feel the industry shares your view of risk?

HJG: You will need to ask them. However, I observe growing awareness in general, and in detail questions around accuracy and bandwidth of offered threat intelligence data as well as understanding of cyber modelling approaches. Boards start to recognise that this type of exposure, due to its virulence, requires top management attention and will be a D&O matter should their companies suffer from a significant downside following an outsized, unmanaged loss scenario. Besides boards, regulators (e.g. EIOPA, PRA, MAS, BAFIN), policy makers including governments and ratings agencies, start to focus on the virulent nature of cyber exposures, its potential management and, most importantly, implications for the reinsurance industry.

Will all this effort serve a relevant market space?

HJG: Clearly, yes. According to various sources, the affirmative cyber insurance market globally is expected to hit the $14bn mark by 2022 from less than $7bn today. The reasons for the rapid premium growth include: An exponentially increasing number of cyber-attacks; a rapidly growing number of IoT and IIoT devices and related vulnerabilities; global enhancement of regulations or directives on personally identifiable information loss (like GDPR, CCPA, etc.); increasing awareness of cyber thefts among small- and medium-sized enterprises providing digital services; a growing number of companies viewing cyber security insurance as a risk-mitigation strategy.

Sounds all extremely attractive. There is risk, there is demand for cover and there is an industry willing to conquer the challenges. But there seems to lurk around a threat of its own. What is it?

HJG: Many specialists are concerned about cyber pricing. But the wrong price won't kill you straight away. Missing risk accumulation will. And my concern is around silent cyber and its way through the value chain from risk via insurance to reinsurance. The following thoughts serve illustrative purposes and numbers can be challenged but directionally they are pointing to the issue.

Global non-life insurance premium accounts for $2.4tn. About 17% or $400bn are property premium. If we assume a worst-case, silent cyber loss could stack up to 5% loss ratio on property premium, this translates into a $20bn silent cyber loss. Given existing property risk reinsurance structures it is reasonable to assume that 90% of this loss ($18bn) will run down into reinsurance. Be reminded of the Thailand floods and how a large event made its way through uncapped risk covers into reinsurance. An $18bn reinsurance loss translates into 3.5% to 4.5% of global reinsurance capitalisation, which is estimated at $400bn-$500bn. A loss of $18bn may look small compared to reinsurance capital resources, but is significant because it is outside yet managed loss scenarios and therefore runs against the reinsurance industry's excess capital which was recently estimated by S&P for the global top 20 reinsurers at around USD20bn

PH: This perspective underscores the immediate need for risk management and modelling capabilities to focus on silent and then to shift this capability immediately on affirmative cyber exposures. This is the only way to keep the industry's loss resilience to the highest standards it has proven so far.

HJG: That's why we believe cyber exposure needs to become a priority for boards and management. We decided to make these client initiatives our focus and developed a proprietary toolbox. We are already successfully engaged in projects with (re) insurers and our support ranges from education, tailored scenarios, wording analytics to potential loss quantification.