Cyber risks – The stakes are high for reinsurers

Peter Hacker, cyber security expert and public speaker and **Hans-Joachim Guenther**, reinsurance and risk expert, share their thoughts on cyber risks and develop a framework for the global impact on the reinsurance Industry.

From boring bog-standard peril to a virulent challenge

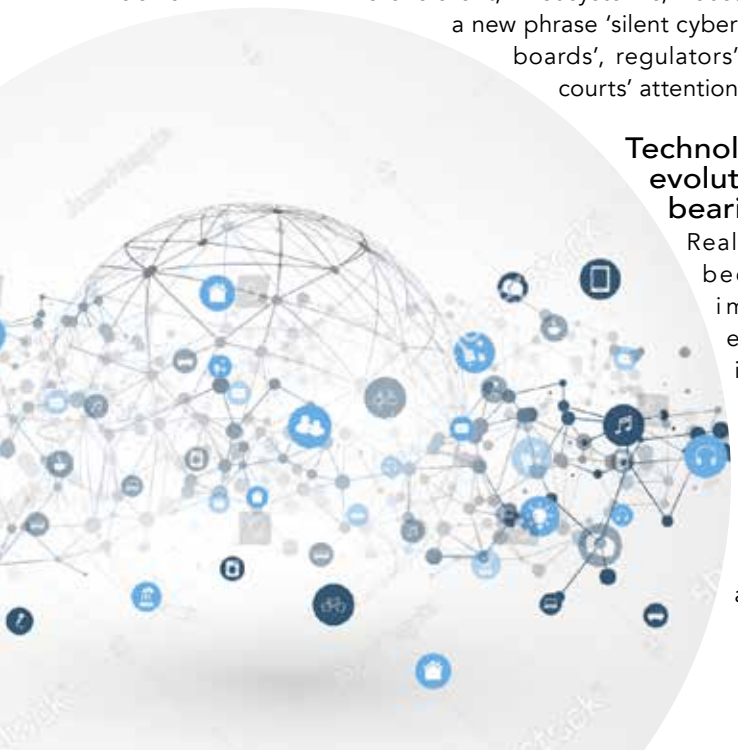
Cyber risk has a history. It started in the '70s as electronic data processing insurance covering losses following computer breakdown and costs related to data recovery. Cyber risk appeared for the first time in the late '90s when the industry became aware of system glitches in software that could not handle the year number 2000.

Around 2003 we had the first named perils based on standalone privacy breach or network security failure endorsements and, soon after, cyber policies emerged primarily meeting US data directives demands.

In 2007-2008 the global financial crisis drew attention to other areas of the insurance industry. Nevertheless, development of standalone cyber products accelerated from 2009 onward – with the main focus still on the US - while the rise of technology errors and omissions (E&O) policies started in the London market.

Moreover, accelerating coverage demands in CTM business led the way to the first wrongful act based 'all risk' technology E&O policy. This arrangement extended into first- and third-party cyber perils. Consequently, the cyber market reacted by broadening existing first- and third-party cover again which resulted in exponential premium growth and profitability in the USA.

In mid-2017, we got the first wake-up call after significant cyber-attacks (WannaCry and NotPetya). These started a renaissance that recognised cyber risk as a more relevant, if not systemic, industry challenge. Moreover, a new phrase 'silent cyber risk' appeared and got boards', regulators', rating agencies' and courts' attention.



Technological (r) evolution and its bearing

Real-time connectivity is becoming increasingly important. Perfect examples are just-in-time supply, order anticipation, stock optimisation, predictive maintenance and incident/accident forecasting. This list is growing day-by-day and myriad applications will be developed ultimately to push existing and new business models forward but at unparalleled competitive margins.

Initially, connectivity will be a competitive edge but quickly become core to survival. One of the magic phrases is the internet of things (IoT). Take our personal lives. Just a few years ago we used the internet only from fixed devices but very soon 90% of our internet traffic will be from mobile devices. In a few years, a real big 'thing on the internet' will be cars and autonomous driving opening a new dimension of cyber exposure. In the next few years billions of IoT devices will be used in businesses globally.

Company values are less and less dependent on tangible assets and more dependent on intangible assets such as IP, reputation, brand, knowledge and customer data. Some call this (r)evolution disruption, but it is ultimately (r)evolution driven by the latest technology. And it does not just serve pure business reasoning, but helps ethical, environmental or resource-saving ambitions that are of the utmost importance in our densely-populated world.

Cyber risk nature

Looking at this picture explains why we became vulnerable to cyber incidents affecting our lifestyle and business connectivity, based on malicious acts (crime) or non-malicious acts (E&O).

It does not take much to see that increasing connectivity and increasing value of intangible breeds a new class of crime: Cyber.

Cyber attacks are unique in two ways: They are global and so writing a global portfolio of cyber risks isn't diversified like Nat CAT; and they are manmade. They are driven by criminal minds, stealing knowledge, IP and money or destroying and disrupting lives.

State-sponsored attacks are worse as they seek to infiltrate or damage entire economies. State-sponsored attacks focus on materially important companies, critical infrastructure including healthcare and utilities, provoking contagious effects creating a chain reaction through a large number of damaged entities intended to destabilise a nation.

Cyber risk is highly contagious. Contagion is not new to our industry but there are major differences with cyber. It's the way this exposure spills into (re)insurance. The relatively young practice of affirmative cyber covers almost serves like a primary layer next to existing policies which could respond to cyber losses on a non-affirmative ('silent') basis.

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.

There have been always situations when new risks were recognised as uninsurable e.g., BI, contingent BI or environmental impairment covers. However entrepreneurial vision, careful risk management and multidisciplinary knowledge pooling allowed for those boundaries of insurability to be moved. Progress often came along with some painful lesson before the product became sustainable, e.g., D&O. All insurance innovation has a link in common: It is driven by demand for coverage. Cyber insurance follows this pattern.

Cyber risk management

Demand is growing and insurance is responding. This situation is much like running before you can walk properly. Irrespective of type – state-sponsored or criminal – cyber exposure will be challenging when it comes to insurance modelling. Nat CAT are based on acts of God with manageable trend risk during contractual annual (re) insurance terms and allow for decent proxy from experience. Cyber exposure will require more complex methodologies and cannot be built on experience because of its man-made criminal dynamic.

The current dualism between affirmative and silent covers aggravates the challenge. It is like an iceberg. The visible part (affirmative) is already dangerous but the invisible part (silent) underneath the surface could be disastrous.

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. Cyber exposures and the relevance of contract wording language requires the development of bespoke modelling approaches which combine qualitative with quantitative aspects.

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.

Positive momentum derives from growing awareness and more detailed scrutiny of accuracy and bandwidth of offered threat intelligence data as well as modelling approaches. Boards are beginning to acknowledge that the virulent nature of this exposure requires top management attention and will be a D&O case should they suffer from a material loss following an unmanaged stress scenario.

Regulators, policy makers, governments and ratings agencies are also shifting their attention to the virulent nature of cyber exposures, proper risk management and, most importantly, to the downstream effects on the reinsurance industry.

Cyber risk is sizeable

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: (1) an exponentially increasing number of cyber attacks; (2) a rapidly growing number of IoT devices and related vulnerabilities; (3) global enhancement of regulations or directives on personally identifiable information loss (like GDPR, CCPA, etc.); (4) increasing awareness of cyber thefts among small- and medium-sized enterprises providing digital services; (5) a growing

number of companies viewing cyber security insurance as a risk-mitigation strategy.

As result of our own and proprietary cyber risk scenario analytics, global economic losses will range between $121bn and 234bn and insurance losses between $27bn and $40bn. These scenarios include a massive power outage or a major cloud operation and domain name server failure resulting from a coordinated global cyber attack, using the combination of a high volume and intensity-driven distributed denial-of-service attack with between two and four attacking vectors, one of them a major ransomware backing a wiper.

The worst scenario is built upon a combination of both. The insurance claims would split into 16%-20% for 'silent' components (property damage, business interruption, marine and liability) and approximately 80%-84% for affirmative coverage elements (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.

Cyber risk can wipe out major portion of global reinsurance excess capital

Many specialists are concerned about cyber pricing. But missing risk accumulation would be immediately fatal and the proper concern – at this stage - must focus on silent cyber throughout the value chain, from risk via insurance to reinsurance.

Let's play around with a few numbers for illustrative purposes. 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.

In its latest reinsurance highlight 2019, S&P estimates an excess capital of about $20bn for the leading top 20 reinsurers. The conclusion is: Silent cyber has the power to wipe out a substantial amount of the global reinsurance excess capitalisation which is the foundation of the loss-resilience profile of this industry. No doubt cyber exposure needs to become a top priority for boards and top 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.

Summary

At this moment cyber is the most underestimated risk of our industry. And it's no longer a black swan because too much is already known.

Cyber risks have an unparalleled and unique risk nature and challenges. The stakes are certainly high for both the reinsurance and direct insurance industry. Without a managed risk approach to cyber exposures, reinsurers and insurers are severely exposed and could suffer from outlier losses, eventually causing reputational harm and unforeseen financial losses.

Cyber is different from any other current insurable peril. Cyber is a truly global exposure, fully manmade and driven by criminal energy. Due to its nature, diversification is much less achievable than in other lines of business. These ingredients carry huge potential for large aggregate losses as a single event might trigger many independent policies.

Cyber exposures will most certainly grow due to the increasing vulnerability of our social and economic life. The driver behind this trend is the massive growth in number of interconnected devices which are all capable of being compromised.

Many existing policies in property and other lines of business do not exclude cyber properly and therefore cover may be triggered for a cyber event irrespective of whether such coverage was intended, or any premium was charged (silent exposure).

This leads to increasing attention at board, regulatory, rating and policymaker level. All these stakeholders have in common a material demand for transparency in respect of size of potential losses.

Cyber models will be bespoke and based on qualitative and quantitative assessments fully to reflect the individual contract wording(s) situation.

Over the next few years the gap between economic losses and insured cyber losses will shrink rapidly and cyber will represent a loss exposure which is on a par with the worst Nat CAT losses but with a potential return period that is much shorter than in Nat CAT scenarios. Companies that recognise and address such developments early will thrive in this new age of intangible risk. Others may well falter.