Maintaining insurers' relevance in the digital age

Dr Kai-Uwe Schanz of **Dr. Schanz, Alms & Company** argues that in order to maintain its relevance the insurance industry must come to grips with cyber risk.

Cyber risk is arguably the biggest challenge facing modern digital economies. It encompasses a multitude of risk sources threatening the information and technology assets of firms, governments or individuals.

The spectrum of risks includes identity theft, disclosure of sensitive information, and business interruption. Non-criminal sources such as power outages or technical or human failure have to be distinguished from criminal sources (cyber crime), including physical attacks, hacker attacks and extortion.

Estimating the costs of cyber incidents is challenging. Some studies put the annual economic cost of cyber incidents at up to US$500 billion, 0.7% of global GDP – a figure well in excess of average annual economic costs associated with global natural disasters.

Current annual gross premiums for global cyber insurance are estimated at around $3–3.5 billion, about 1.5 permille of global non-life premiums.

Some experts expect the global cyber insurance market to grow to $20 billion by 2025 which would be still considerably less than 1% of the global non-life market.

A yawning protection gap

A comparison of the aggregate global damage from cyber incidents with the cyber premiums generated by the insurance industry suggests that virtually all cyber losses remain uninsured and, from a macro perspective, insurance-based transfer of cyber risk is virtually irrelevant.

Lloyd's recently attempted to quantify the cyber risk protection gap for two specific scenarios – a cloud service provider hack, leading to widespread service and business interruption, and a mass vulnerability attack, as a result of leaked information which is used by criminal parties to attack vulnerable businesses for financial gain.

For the cloud service disruption scenario, estimated economic losses range from $4.6 billion for a large event to $53.1 billion for an extreme event.

In the mass software vulnerability scenario, the losses range from $9.7 billion for a large event to $28.7 billion for an extreme event – similar to the economic losses caused by a major hurricane.

Only a small fraction of such losses would be indemnified by cyber insurers. Under the cloud services scenario, the cyber risk protection gaps (uninsured losses as a share of total losses) would come in at 87% (large loss) and 83% (extreme loss), respectively.

The gap is even larger for the mass vulnerability scenario and is estimated to reach around 93% for both the large and the extreme loss event.

Insurability challenges

The concept of insurability helps with the understanding of the fundamental constraints facing cyber insurance.

A first insurability challenge is the lack of independence and predictability of cyber losses. As a result, risk pooling hits its limits. Exposures are largely unpredictable not only because of a lack of data (which is set to accumulate over time) but, more fundamentally, in light of the dynamics of cyber risks and the associated risk of change which complicates risk assessment.

A second insurability challenge in cyber insurance is asymmetric information. Adverse selection is almost inevitable as organisations that have experienced cyber incidents before are more likely to buy insurance. The lack of loss data impairs risk classification of policyholders which renders adverse selection even more acute. The lack of historical data is arguably the most fundamental challenge and contributes to tight coverage limits in cyber insurance markets.

Tackling the challenges

Despite the many challenges to the insurability of cyber risk, one should bear in mind that the cyber insurance market is still at an embryonic stage. As the market matures, risk pools and relevant data sets will expand. New players will grow the market's capacity.

In addition, policy wordings and product specifications will see more standardisation.

And, last but not least, the fundamental issue of insurability could be addressed by public-private partnerships in order to develop a robust commercial market for cyber risks.

Arguably, cyber, as a genuinely global risk, presents the insurance industry with a fundamental strategic challenge that could even prove to be existential. The product suite and risk appetite of insurers increasingly fall short of the pace at which the digital economy of the future emerges.

Let us all join forces to prove those pessimists wrong who contend that insurers are set to lose their relevance to society if they fail to make more meaningful contributions to the protection of the virtual space of economies and societies.

Dr Kai-Uwe Schanz is Chairman of Dr. Schanz, Alms & Company AG, Zurich. He can be contacted at kai-uwe.schanz@schanz-alms.com.