Single coordinated cyberattack could cause $40bn insured losses, hammer global reinsurance surplus and hit captives

By Adrian Ladbury on November 6, 2019

The growing focus of insurers and reinsurers on the potentially catastrophic impact of so-called silent cyber cover held within traditional policies is fully justified, because a single coordinated cyberattack could significantly reduce the surplus capital base of the world's leading reinsurers and may massively reduce risk appetite, according to experts.

Peter Hacker, cybersecurity expert and public speaker with experience of working in structured reinsurance and technology insurance, and Hans-Joachim Guenther, reinsurance and risk expert, as well as former executive board member and chief underwriting officer at various large reinsurance companies, have developed their own proprietary cyber risk scenario analytics. They believe that a single attack could cause economic losses of up to $234bn and insured losses of up to $40bn.

The reinsurance sector would take the lion's share of the silent cyber losses within that total. Captives might well take a material hit primarily from embedded silent cyber exposure in P&C lines, according to the analysis, which was released at the recent Singapore Insurance and Reinsurance Conference.

Mr Hacker, who recently held a session on this topic at the Swiss association of Insurance and Risk Managers (SIRM) annual conference, explained: "As result of our own and proprietary cyber risk scenario analytics, we believe global economic losses can range between $121bn and $234bn, and insurance losses between $27bn and $40bn. The scenario is based on a massive power outage or major cloud operation and domain name servers failure resulting from a coordinated global

cyberattack, using the combination of a high-volume and intensity-driven distributed denial-of-service attack (DDoS) with two to four attacking vectors, one of them a major ransomware backing a wiper. In the broadest sense, we talk about DDoS plus NotPetya/WannaCry alike, but without a subsequent 'quick' kill switch and with broad interruptions of three to seven days across numerous sectors and company sizes," he told *Commercial Risk Europe*.

"Over the next few years, the gap between economic losses and insured cyber losses will rapidly shrink and cyber will represent a loss exposure that is comparable to the worst natural catastrophe losses but, significantly, with a potential return period that is much shorter than in natural catastrophe scenarios," continued Mr Hacker.

Mr Guenther added that, at this stage, a prudent estimate for silent cyber loss would probably account for about 20% of an insured loss, though he did add that this assumption may well change once pending court cases are resolved. However, he said it is important to note that if data is considered a physical, tangible asset, or non-kinetic warfare such as state-sponsored cyber warfare activities are not, or only partially, excluded, the 20:80 split could exponentially well change, resulting in massive pressure on conventional P&C markets.

"Given existing property and casualty risk reinsurance or captive structures, it is reasonable to assume that 90% of this loss will run down into reinsurance. Be reminded of the Thai floods of 2011 and how a large event made its way through uncapped risk covers into reinsurance. Silent cyber losses are mostly outside managed loss scenarios and therefore running against the reinsurance industry's excess capital," he said.

"Standard & Poor's states in its latest *Global Reinsurance Highlight 2019*report that the leading top 20 reinsurers have excess capital of about $20bn to $30bn. The straight conclusion reads: 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. The threat related to silent cyber is pretty much the same for captives, which will need to carefully assess their silent cyber exposures against their limited capital," added Mr Guenther.

Mr Hacker agrees with a rising body of regulators and experts in the risk management and transfer sector that this potentially catastrophic risk cannot be managed in isolation. It needs a joined-up approach.

"Cyber risks are simply too complex to be handled in isolation. No matter what capital size the (re)insurance parties can offer, it is a challenge that needs to be addressed top-down by regulatory bodies, the (re)insurance industry, capital markets, cybersecurity vendors and corporations together. Personally, I remain convinced that broader solutions backed by governments, (re)insurers and capital markets, such as cyber risk transfer pools or ILS structures, will be mid- to long-term products to manage huge loss scenarios. In any case, nobody can afford running continuously with such a high degree of potential silent cyber exposure," he said.

But while governments, regulators, industry associations and the like work out how best to tackle this problem, individual risk managers within corporations, insurers and reinsurers need to take a good look at their exposure, how and whether they are covered, and revise their response and crisis management plans sooner rather than later.

The Swiss experts have already carried out education, and reviewed coverage wordings, exposures and potential accumulations for a number of risk managers within both corporations, captives and the (re)insurance sector. Demand will clearly rise for such expert, third-party assistance.

Mr Hacker said corporate customers should run board simulations that stress-test their readiness to respond to critical cyber incidents and help verify the appropriateness of insurance solutions. But these need to be truly dynamic tests, not tickbox exercises, he stressed.

“This cannot be done with simple table desk exercises or ‘card games’. This requires a dynamic and non-linear simulation that reacts to the way management responds to an incident. [Being] forced to decide under stress is different to working [from] a handbook,” he said.

Mr Guenther added: “Always think of your cyber exposure under the assumption that it is not a matter of ‘if’ but rather ‘when’ an incident will occur. This is crucial for your cybersecurity policy, but also important when structuring an affirmative cyber policy. Severe cyber claims tend to increase during 12 to 18 months as the full impact is often not seen when the incident happened. The first three to six months mostly focus on incident triage – discovery, disclosure, forensic and criminal investigation phase. This is followed by nine to 12 months’ broad impact on management time to facilitate business recovery internally as well as externally. Incident management skills and top management preparedness for crisis situations are fundamental prerequisites for minimising the impact of cyber Incidents.”

Mr Hacker agreed that risk managers need to keep a close eye on costs. However, the fact that some unintended silent cyber coverage exists between contracted parties is no reason to expect that coverage for a new and extremely complex insurance can be obtained for free or even cheaply, he said.

Put simply, the silent coverage situation must be resolved sooner rather than later, as it carries significant uncertainties about scope of insurance protection.

“Industry concerns about silent cyber certainly are justified,” said Mr Hacker. “Many existing policies in property, casualty and other lines of business do not properly exclude cyber – malicious and non-malicious – and therefore are exposed to respond to a cyber event irrespective of whether such coverage was ever intended, or any premium was charged. This ambiguity needs to be urgently removed. It is like an iceberg. The visible part –affirmative – is already dangerous, but the invisible part – silent – underneath the water surface will cause a disaster rather sooner than later. Cyber remains an emerging, ‘known unknown’ and possibly pandemic-like exposure that causes massive headaches around contract certainty across corporate insurance customers and (re)insurance boardrooms,” he added.

According to survey findings revealed at *Commercial Risk Europe*’s latest event, **politically motivated cyberattacks cause the most severe disruptions of all geopolitical risks** for organisations across the world. The survey also found that only a quarter of firms polled buy political risk insurance, with the majority saying it is more efficient to manage the risk internally.

CRE Newsletter, **IPN Newsletter**