Beazley Logo

Article

Leaders need to lead on catastrophic cyber

January 13, 2023

Hospitals unable to access patient data, bank transactions paused and destructive breakdowns in utility services, such as broadband, or the supply of basics such as running water. This is the kind of havoc that a catastrophic, prolonged cyber attack could have on the smooth running of society and the economy.

As the world has becoming increasingly digitized and interconnected the potential for the outage in one of the lynchpin elements of the economic and social architecture has moved from the realms of science fiction to reality.

As a leading cyber insurer it is our job to think hard about how we address these scenarios - whilst it thankfully remains only a possibility. To date the largest cyber attack events, even widespread ones such as ‘WannaCry’ or Log4j have impacted individual organisations and corporations with limited system wide implications. Whilst we know these can have significant consequences for those directly impacted within those organisations - their staff, customers or patients - the wider world has largely been spared.

With this front of mind, we have been working hard to address the unthinkable and identify realistic catastrophic scenarios that would so upset the economic and/or social fabric that they could also majorly disrupt the commercial insurance market.

Let me be clear, in Beazley’s opinion most cyber events, even systemic ones, are insurable and should remain so. With a large book of cyber business, around $ 2billion GWP, we have an excellent handle on our own exposure and the potential damage that a catastrophic event could cause to the whole market.

So why is this important to us? As one of the largest insurers in a competitive market why not just continue our growth trajectory, protecting our own book from harm, looking after our clients and build out a very successful cyber business?

The truth is that as a market leader we believe we have a duty to lead - so that the market can evolve in size and scale and clients can get the protection they need.

Sometimes, more really is more

Independent estimates suggest that by 2028 the cyber market will have grown to $37 billion , and our own assessment confirms this. We believe growth at that scale is realistic, given the threat is growing every day and business desperately needs protection.

Demand for a high quality, responsive cyber insurance product, that not only pays out should the worst happen, but as importantly offers pre-attack mitigation services and post event recovery support continues to grow exponentially. But to deliver this we need to attract more capital into the market and see the size of the total market expand at the same rate and pace as demand is growing.

Beazley wants more capacity in the cyber market, more carriers, more product innovation and more reinsurance capacity from both trade and third-party capital providers.

So how are we proposing that we build the capacity in the market and deliver to clients and brokers the depth and breadth of cover that they deserve?

A three-part solution

Firstly, we are addressing the challenge of cyber catastrophes head on by defining the two scenarios that could trigger the most substantial economic or social dislocation. They are a prolonged outage of a major Cloud Service Provider exceeding 72hrs; or contagion malware in a Computer Operating System, causing a major detrimental impact to a state’s essential services. These two triggering events would still be covered with full access to our cyber services to recover from attack but a 50% sub-limit of insurance would apply. Defining these events will enable us to model the exposure, give capita providers the confidence to commit to the long-term future of the cyber market and deliver peace of mind to clients that they are protected in even the most extreme scenario.

And finally, we’re actively clarifying the war exclusion, making it fit for the 21st century. War is not insured as standard in any cyber insurance policy and since the start of the Ukraine war in February 2022, the need for clarity on how cyber fits into an overall war situation has become urgent. Where a full blown, state on state situation of war exists, including the use of cyber-attacks as part of war, or if state-backed cyber-attacks cause major detrimental damage to essential services in another state, they fall under the war exclusion. Individual state attacks outside of a state of war, which do not cause major detrimental impact to essential services, remain covered under existing cyber policies.

Collaboration is key to increasing capacity

We’ve worked on this solution collaboratively with brokers, reinsurers, market associations, regulators and law enforcement – and they have all been supportive of our efforts. By clarifying the wordings around

catastrophic cyber, infrastructure and war, Beazley has created a clear and understandable operating framework for addressing a complex and fast-moving subject.

This is about achieving a balance between the sustainability of the product and the market and recognising that insureds need coverage for even the most extreme scenarios within their cyber insurance policies.

By establishing a reasonable ceiling for what the private market or any one insurer can withstand when faced with a cyber attack, my hope is that we will encourage more capital to the market so it can continue to meet the growing cyber risk needs of business everywhere.

1 Cyber Insurance Market Size Worth USD 36.85 Billion by 2028 (globenewswire.com)

Home

©Beazley Group | LLOYD's Underwriters