beazley

Article

The next test for cyber insurance

Paul Bantick • July 12, 2023

Russia's invasion of Ukraine is providing the insurance market with a demonstration of how warfare has evolved. Predictions that cyber-attacks would form part of the arsenal of any modern aggressor have come true. For example, through digital means, nation states embroiled in conflict can now strike at critical infrastructure in novel ways, beyond the range of, or shielded from, their missiles and bullets. Cyber-attacks on computer systems, coordinated to strike at critical infrastructure essential to a country's functioning, can have a devasting impact.

I spend a lot of time discussing cyber war at the moment, and in our latest Risk & Resilience survey it is no surprise that war in all its guises now concerns nearly a quarter (24%) of the 2,000 global businesses leaders we surveyed, fearing that it is a risk they will face one day. Traditional warfare has been excluded from most insurance policies, as markets recognised that it is too big a risk to cover. Now cyber is also a tool in nation states' arsenals, it is recognised that cyber war is similarly too big a risk for the cyber market to cope with.

Russia-Ukraine conflict demonstrates the use of cyber as a nation state weapon

In the first three months of 2023, according to the Security Service of Ukraine's (SSU) Cybersecurity Department, Russia was responsible for almost 1,2001 cyberattacks and other critical cyber incidents. Russia knows that cyber-attacks are a central pillar of its war effort. Damage caused so far has largely been contained to Ukraine but as capabilities evolve, so too does the risk of global 'contagion' across numerous platforms that could impact numerous organisations who get caught up in the virtual 'crossfire'.

Lloyd's noted last year2, the damage that a cyber war attack can cause and its ability to spread creates a potential systemic risk to insurers. The evolution of the capabilities of a nation-state to use cyber as a means of warfare has been demonstrated by Russia, and showed the role which cyber can play in future conflicts in a way that was not technologically possible in the past. When war exclusions were originally drafted, this development could not have been predicted.

Why would the insurance industry not also evolve to reflect this?

Creating a cyber war market

How can we help clients? First, we need to be very clear on the cover that we are and are not giving. Second, we need to continue to help our clients build their resilience to cyber risks in all forms, as the art of cyber incident survival is to have the best possible resilience measures in place should you be impacted by a cyber war event. Third, we are working in collaboration with other insurers, brokers and the Lloyd's Lab to develop a dedicated cyber war product to provide some cover in the event of a cyber war event, and we hope to launch it soon.

It is clear businesses now feel more exposed to the risk of cyber war. We must provide a solution to address our clients cyber war exposure should they wish to. Most importantly, we must do so together. The insurance industry has a long history of affecting positive change through collective action. By collaborating at this key juncture for the cyber insurance market we can offer insureds clarity and certainty when it is needed most.

The cyber insurance market has come of age in recent years and is predicted to triple in size over the next three or four years. This progress is a testament to the work of every cyber underwriter and broker: we have built a robust market, proved its viability, highlighted its worth to insureds, paid the claims and stood firm on pricing when needed.

Now we are evolving again. Cyber war and how we create a new market for this peril is the next test for our class, we can fail individually or pass collectively.

Paul Bantick

Chief Underwriting Officer

1 https://www.digitaljournal.com/world/terror-at-the-click-of-a-mouse-russias-cybersecurity-war-continues-to-unfold/article

2 https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

beazley