Cyber, conflict and cover: time for a re-think?

Published 11 September 2018

The debate about the boundaries of cyber policies cuts right across the insurance industry's strenuous efforts to raise awareness of the need for cover and the availability of a growing range of solutions. Just as many more businesses look to the insurance market to protect them, the market is starting to raise warning flags over issues around aggregation and systemic risk.

Many businesses are ill-prepared for the potential impact of major cyber-attacks, with smaller firms often believing they are too small to be a target. This leaves them vulnerable because they frequently do not put the policies, staff training and technical measures in place to protect themselves and do not buy the insurance protection that would provide them with the right indemnification and support when an attack comes.

This is a common problem around the world, says Dr Maya Bundt, Head of Cyber & Digital Solutions at Swiss Re. "Many smaller companies are still not aware of the true nature of cyber risk that has crept into their business model as the flip side of digitisation. An often-heard argument from the industry is that their small size precludes businesses from being targets. Unfortunately, this is not true. Smaller companies can be hit by a wide-spread or large-scale cyber event just the same as larger companies. In fact, they might even be less prepared and more vulnerable."

Awareness of the need to take cybersecurity seriously and insure against the consequences of attacks and data breaches was given a major boost by the arrival of the General Data Protection Regulation (GDPR) in Europe at the end of May. This not only helped push cyber risks up the boardroom agendas of European business but has had a significant impact elsewhere.

In Australia, mandatory reporting was introduced in February this year and is already having an impact. "Even though mandatory reporting was introduced in February, GDPR is prompting Australian companies, especially those with customers in Europe, to look at adopting an even stricter regime. This could prompt an earlier than expected review of current legislation," says Kieran Doyle, Special Counsel at Wotton + Kearney, Australia, a Legalign Global partner.

"Other jurisdictions are having to adopt GDPR procedures if they have significant business relationships in the UK and Europe. In New Zealand, export-driven businesses are likely to be ahead of the game and need to be right on top of what GDPR requires of them," says Mark Anderson, Partner at Wotton + Kearney, New Zealand.

Exposures have grown much wider than protecting against the typical data breaches, phishing, malware and ransomware attacks that are almost an everyday occurrence for businesses. Major incidents such as last year's worldwide cyber-attack by the WannaCry ransomware crypto worm dispelled a lot of complacency about the potential for attacks to propagate and have a serious impact on a wide range of businesses in the highly connected world of modern commerce.

This creates a potential "shrapnel effect," says cyber expert Hans Allnutt, Partner at DAC Beachcroft, in which businesses far away from the centre of an attack suffer. "It is easy to rationalise a cyber-attack that is focused on your business system or data, but when you see things happening in your system that does not seem to be focused on your business, this might be the shrapnel effect. You are not the original target of the attack, but you get affected by it."

Covering this risk means taking a much broader view of the range of business interruption (BI) cover businesses require, a trend that is already running strongly in the US, says Gregory Bautista, Partner at Wilson Elser, USA, a Legalign Global partner.

"Many companies are increasingly concerned with potential BI losses triggered by cyber events such as the global WannaCry and NotPetya attacks last summer. These incidents have made cyber BI coverage more relevant from a buyer's perspective. As property and other traditional insurers seek to reduce their potential exposure for cyber-related losses, cyber insurers, in turn, have begun expanding their policies to include BI and contingent (third-party) business interruption (CBI) coverage resulting from cyber events or attacks. These BI losses can dwarf any potential privacy losses arising from a loss or theft of personal data."

His colleague Anjali Das, Partner at Wilson Elser, says the market is responding to this by extending the cover that is available. "Increasingly, CBI coverage is being offered in some cyber policies, which protects companies which depend on third parties for their operations from cyber-attacks on those third party providers. CBI coverage anticipates third-party supply chain disruptions that may have a significant adverse impact on an insured's operations. Recently, we have in fact seen an uptick in cyber claims reported by an insured originating from an attack on one of their vendor's computer systems or networks."

While the extension of cover to protect against the 'shrapnel effect' will accelerate, preparing and protecting against attacks will get harder as the techniques used by criminals constantly evolve. If that is not already a big enough challenge, identifying the source of attack is getting harder too, says Allnutt. “The methods of attack are quite wide-ranging and the people who are motivated to carry them out are increasingly diverse too. They could be states, criminals, terrorists, activists – or just a renegade with some basic technical skill.”

For the insured who has bought cyber cover they just want the insurer to move quickly to help them mitigate their losses and get back to normality as quickly as possible, secure in the knowledge they will indemnify them against the losses suffered: “The policyholder doesn’t want a lot of questions about whether a terrorist or a malicious individual was behind the attack,” says Allnutt. "They will just want their cyber losses insured.”

The challenge for policyholders now is that insurers are looking for greater clarity and will need to ask precisely those questions. The answers might determine whether – or to what extent – the policyholder is covered, adds Dr Bundt.

“Until a few years ago cyber business was written with both war and terrorism exclusions. Mostly due to the difficulties in defining and proving cyber terrorism and the fact that insureds have a strong need for protection and contract certainty, terrorism exclusions have largely vanished for cyber business,” she says. “In fact, different jurisdictions have been reacting in different ways to deal with terrorism risk. For example, Pool Re in the UK has explicitly included property damage resulting from cyber terror attacks into its scope.”

There are no easy answers to questions around the definition of terrorism, says Bastian Finkel, Partner at BLD Bach Langheid Dallmayr, Germany, a Legalign Global partner. “It all depends on the question of what exactly I want to insure. If I want to exclude war or – more relevant – terrorism risks, I must be clear about the definition of terrorism. Will this only be defined by the subjective goals of the terrorist or, alternatively, also by objective criteria regardless of the terrorists’ motivation? In our experience, the cyber world knows different forms of terrorist-like acts, although they might not fulfil criteria of classical terrorist acts. Maybe such a distinction must be ignored in the cyber-insurance world. That, of course, would lead to a broader coverage.”

Allnutt says the question now being debated among cyber underwriters is how to define the scope of their cover and to whom they offer it so as to limit the potential for aggregation. “There is a fear of aggregate systemic exposures among insurers,” he says. “This is leading some of them to question the current definitions and scope of cover. We know that the physical risks from war and terrorism are too large for individual insurers to cover and that market solutions such as Pool Re have to be put in place. It is time to look at definitions of conflict in the age of cyber too as, indeed, Pool Re has done by extending its cover beyond physical damage.”

This is far from being a UK problem alone but the solutions are going to be hard to define, says Dr Bundt: “In times of cyber conflict, the picture has become even more challenging, the main reason being that it is very challenging to attribute cyber-attacks to a certain actor. That makes it also extremely difficult to decide if a cyber event is, in fact, an act of terror or not. One example here is the apparent terror attack on the French TV network tv5, which later turned out was not performed by ISIS, but by a well-known group of Russian hackers.

“For the insurance industry this means that trusted mechanisms like airtight exclusion language do not work anymore,” she concludes. “We need to find ways to safeguard both potential victims of such an attack and the insurance industry as a whole.”

The challenge of reconciling those two laudable objectives is going to draw the insurance industry into another debate about its role in modern society.

UK insurers need help to determine and price cover but may step away from conflict cover

Joe Ahern, policy lead for cyber insurance at the Association of British Insurers (ABI), told a recent event hosted by the Centre for the Study of Financial Innovation (CSFI) that insurers needed more help from the Information Commissioner’s Office (ICO). In particular, he said the ICO must share more information about data breaches with insurers.

The ABI has called on Government and the ICO to allow insurers access, in a secure and anonymised way, to data from the mandatory breach reporting requirement under the GDPR. This, says the ABI, would provide a valuable source of data for insurers to assist them in assessing and pricing the risk of potential customers and enable insurers to offer broader and more tailored cover to firms of different sizes and sectors. The ABI says it has support from Government for this proposal and will continue to make its case to the ICO.

The issues around the extent of the commercial market to continue to offer coverage without exclusions for war and terrorism was also raised at the CSFI event. The ABI says that if the market is to continue to evolve sustainably, insurers may look to exclude damages emanating from attacks on critical national infrastructure, war and terrorism. This would be intended to mitigate against aggregation risk arising from cyber-attacks and is in line with insurers’ responsibility to the Prudential Regulatory Authority to manage exposures prudently.

Global reinsurers share this concern according to Dr Bundt: “Insurance and reinsurance companies need to measure and manage their exposure to cyber accumulation carefully. Also, for very large events that are too big to be borne by the insurance industry alone, it might make sense to find additional risk-sharing arrangements in public-private partnerships or with capital markets.”

Australia could extend terrorism cover

In Australia, many cyber offerings from local insurers provide cover for cyber terrorism rather than exclude it. This is probably due to the

cyber insurance market still developing, albeit at a fairly rapid pace. Additionally, while there is cover under the Australian Reinsurance Pool Corp (ARPC) for declared terrorist attacks for property risks, the same cannot be said for a cyber-terrorist attack so it is important that there is cover in cyber policies for cyber terror, says Kieran Doyle. The ARPC is pushing to review this later in 2018.

Authors

Hans Allnutt
London - Walbrook
+44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com

Mark Anderson
+ 64 9 280 0524
mark.anderson@wottonkearney.com

Gregory Bautista
914.872.7839
gregory.bautista@wilsonelser.com

Anjali Das
312.821.6164
anjali.das@wilsonelser.com

Kieran Doyle
+61 2 8273 9828
Kieran.Doyle@wottonkearney.com.au

Bastian Finkel
+49 221 944027-893
bastian.finkel@bld.de

DAC BEACHCROFT