MARSH

RISK MANAGEMENT | MARKET UPDATE

Cyber Coverage in Property and Casualty Insurance Programmes

Companies will face more restrictive exclusions in respect of cyber coverage within their property and casualty insurance policies.

With cyber exposures generally increasing in recent years, and the insurance market already in transition, some insurers are seeking to limit or even remove computer-related coverage outside of their standalone cyber policies from 1 January 2020.

Companies should engage with their brokers and advisers as early as possible, in order for the broadest coverage available to be negotiated for the best price.

Increased Exposures

With most property damage and business interruption programmes underwritten on an "all-risks" basis, all property damage and resulting business interruption is covered unless expressly excluded. An all-risks property and business interruption policy has many exclusions or limitations, however, including in respect of computer systems and electronic data.

Historically, casualty policies tended to be silent on "cyber" exposures. Some casualty insurers viewed specific cyber exclusions as unnecessary, mainly because casualty policies insure against third-party damage to tangible property and third-party personal injury, and computer data is not tangible "physical property".

Before the rise of social media and the internet of things, casualty insurers did not believe they were significantly exposed to mental injury claims (which are included within the meaning of "personal injury"). However, this is no longer the case.

With advancements in computer technology in recent years – including the proliferation of digital devices and the increased frequency with which they are connected to physical systems – companies have far more cyber exposures.

And with the advent in 2018 of the EU General Data Protection Regulation (GDPR) – with its more stringent scope of liabilities and sentencing provisions than the previous Data Protection Act – any commercial entity potentially has a significant exposure to civil and criminal liabilities arising out of the loss or misuse of data. Additionally, English courts have been ready to find companies vicariously liable for their employees' social media activity[1].

[1] Wm Morrisons Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339.

Regulatory Impetus

The Prudential Regulatory Authority (PRA) – which is responsible for ensuring that insurers are adequately capitalised in order to pay claims – has concerns about how insurers manage exposure to cyber risks. These concerns relate to:

- A lack of cyber expertise within insurers.
- Accumulation issues within cyber policies.
- Non-cyber policies inadvertently providing cyber cover by being "silent" on the issue – that is, not restricting cyber cover within their policies.

In January 2019, all insurers received a letter from the PRA that made it clear that they "should have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover".

Similarly, Lloyd's of London issued a bulletin in July 2019, mandating all syndicates to provide clarity for cyber exposure in all policies. There is a phased approach: By 1 January 2020, all first-party property damage lines of business[2] must clearly affirm or exclude cyber cover; liability policies and treaty reinsurance will follow on dates to be established through 2020/21.

Insurer Responses

Many insurers are responding to this changing risk landscape by seeking to limit computer-related coverage outside of standalone cyber policies.

In support of this stance, the International Underwriters Association (IUA) released two new cyber exclusions that unambiguously remove all cyber-related cover. Meanwhile, the Lloyd's Market Association (LMA) released two more cyber exclusions in November.

All of these clauses would represent a significant reduction in cover for the vast majority of multinational companies.

Early indications are that insurers will favour the LMA clause titled LMA 5400, due to the LMA's reputation and because the LMA clauses are drafted in a similar style to existing exclusions, which insurers are comfortable with.

In terms of coverage certainty, this clause is not in companies' best interests because it introduces a problematic distinction between "malicious" and "non-malicious" cyber events. In the LMA 5400 clause, a non-malicious computer incident is covered only if fire and explosion results, whereas a "malicious" cyber event is always excluded. The definition of "malicious" is exceedingly broad and includes any unauthorised use of a computer.

Transitioning Market

Cyber exclusions vary in property wordings, with all established insurers customarily including a cyber exclusion into their wording. Commonly used cyber exclusions favoured by insurers for nearly two decades are the NM2914, NMA2915, and the CL380.

Neither the PRA guidance nor the Lloyd's bulletin state that these exclusions (NMA 2914/2915/CL380) are inadequate. However, insurers are using the announcements by Lloyd's and the PRA, in the context of an already transitioning insurance market, to impose more restrictive cover from 1 January 2020.

More attempts by insurers to use the new restrictive exclusions throughout 2020 and 2021 are likely, especially if treaty reinsurers adopt a restrictive approach on cyber with their insurer clients. Should this occur, direct insurers will need to impose these restrictions onto their direct policyholders for consistency.

Although different insurers approach cyber exclusions in different ways, Marsh's stance on the issue is clear: We are resisting the inclusion of more restrictive terms, and continue to provide companies with cross-class coverage and placement expertise.

This allows us to design insurance solutions that optimise our clients' coverage, whether that is incidental cyber coverage within the property and casualty policies, or within a standalone cyber policy.

Companies should continue to consider their evolving cyber exposures, and engage insurance brokers who are able to provide expert coverage and placement services.

[2] Energy (both offshore/onshore), nuclear, power generation, cargo, fine art, marine, specie, yacht, difference in conditions, direct and facultative property, engineering, livestock and bloodstock, and terrorism.

CONTACT

FELIX UKAEGBU
Risk management coverage leader, Marsh
020 7558 3724
felix.ukaegbu@marsh.com