bms.

September 2020

London Market Cyber Exclusions

Why the Landscape is changing

In January 2019 one of the UK regulators, the Prudential Regulation Authority (PRA), wrote to insurers[1] calling for more effective management of silent cyber exposures under first-party property damage policies. Silent Cyber refers to the potential confusion under non-cyber policies as to whether "cyber" related risks are covered or not. For years, many lines of business failed to either affirmatively include cyber coverage or explicitly exclude it. This leaves the potential for large scale disputes over whether an insured's data can be considered a tangible asset, and thus covered under a property policy, or whether a cyber attack or administrative computer error that leads to a property damage loss would be covered.

From the 1st January 2020, Lloyd's underwriters have been required to clarify their position on these cyber exposures. Both the insurance and reinsurance marketplace of Lloyd's have mandated that all policies clearly state whether they will provide affirmative coverage and if not, an appropriate exclusion must be applied.

In the wake of this mandate, clients and brokers expected their markets to either:

- introduce cyber exclusions to policies that didn't have them before;
- replace their previous cyber exclusions with more recently developed ones, or;
- reallocate or charge additional premium and offer affirmative cyber coverage.

In preparation for this change the Lloyd's Market Association (LMA) released four new cyber exclusions which aimed to provide greater clarity than their predecessors: LMA5400 Property Cyber and Data Endorsement, LMA5401 Property Cyber and Data Exclusion, LMA5402 Marine Cyber Exclusion, LMA5403 Marine Cyber Endorsement.* More recently, other variations of these exclusions have also been developed which gives the insurer and the insured more choice, but further complicates the topic.

[1] Sweeney, A. (2019). Cyber underwriting risk: follow-up survey results. Available: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results.

*Please note, although called "Property" or "Marine" exclusions, these may be used across any line of business depending on the underwriter's preference.

Property exclusions

The main 'Cyber'/'Data' clauses in use in the London property market were the NMA2914 and NMA2915 and have been in use since January 2001.

Both the NMA2914 and NMA2915 effectively excluded all losses resulting from the introduction of a 'Virus' (as defined in the clause) whether maliciously or by accident, however both of these clauses wrote back 'Resulting Fire or Explosion' as a result of the introduction of the virus.

There was very little difference between these clauses other than in respect of the Electronic Data Processing Media Valuation in Section 2 of both clauses. The NMA2914 allowed for the repair, replacement or reproduction of data as a result of any covered loss from virtually any source reasonably obtained within a required sub-limit, the NMA2915 only provided cover for restoring data from back-ups of the insured's own copies, but without a sublimit.

LMA5400 Property Cyber and Data Endorsement

This clause excludes '**Cyber Loss**' which describes the damage caused by the peril of either:

- a '**Cyber Act**', being the malicious action resulting in a '**Cyber Loss**', or,
- a '**Cyber Incident**', being an accidental or operational error resulting in a '**Cyber Loss**'.

The clause writes back, in item 2, resultant 'Fire or Explosion' directly resulting from a '**Cyber Incident**' only. All other resultant damage remains excluded and there is no 'Fire or Explosion' coverage from a '**Cyber Act**' – i.e. a malicious action.

With regards to data, this endorsement permits coverage for the costs of repair or replacement of the damaged data processing media plus the cost of copying the data from back-ups or from originals of a previous generation. There is no coverage here for research or engineering costs nor any cost of recreating or gathering or assembling the data.

LMA5401 Property Cyber and Data Exclusion

This clause is very similar to the LMA5400 in that it excludes both malicious and accidental cyber events. However, under this clause there is no write-back for any resultant damage following a cyber incident and there is no cover for any repair or replacement of data – it is especially important to note this also means there is no cover for data loss caused by a physical peril such as a fire, explosion, storm, etc. If this clause is applied it is likely to be broader than any previous cyber exclusion a policy may have had.

Marine exclusions

For decades the Marine market (and others) have relied on the CL380 – Institute Cyber Attack Exclusion Clause. The exclusion is short, has a number of undefined terms and continues to raise debate regarding how it should be interpreted. The biggest cause of concern is whether the clause intends to exclude cyber attacks and accidental cyber events, or solely cyber attacks.

This old clause does however address the issue of war, civil war, rebellion, etc., which the property policies fail to do and hence it is usually more suited to Marine policies. Under it, this clause will not exclude cyber events if related to war, civil war, or revolution (etc.) events.

LMA5402 Marine Cyber Exclusion

This new clause is more explicit than its predecessor as it clearly states that both computer failures and cyber attacks are excluded. However, it remains a short clause, lacking in detail, which simply states that any "loss, damage, liability or expenses" related to these incidents are excluded.

Note that this clause does not write back war, civil war, revolution (etc.) events and so is a broader exclusion than the LMA5403 Marine Cyber Endorsement (below). Carefully consider this clause if an underwriter is attempting to use it on a policy which intends to address war.

LMA5403 Marine Cyber Endorsement

The Marine Cyber Endorsement is similar to the LMA5402, however, it does address the issues around war. Here cyber attacks are written back if related to a war, civil war, revolution, etc. event. However, accidental cyber events and operational errors remain excluded regardless. For example, a weapon that is discharged because of an intruder being in a ship's control system would be covered, but had an operational error of the computer system led to the discharge, it would not.

Property coverage gaps

The new exclusions open up a new gap in coverage for those insureds affected by them. Previously, under both the NMA2914 and NMA2915, all resultant Fire and Explosion events would have been covered. Depending on the risk, the broker may have also negotiated other resultant perils to be written back. Now, risk managers should carefully consider the fact they may be completely uninsured for potentially large scale fires or explosions caused by a cyber attack. Under the LMA5401 in particular they will also not be covered if such events were the result of an accidental cyber event.

These events are fewer and farther between than Data losses, but the scale of the disaster can be far greater. One of the most notable events of the past five years is that of a German steel mill that was the target of a sophisticated attack. Perpetrators took control of the mill's industrial control systems, ultimately leading to a loss of control of their blast furnaces. Limited details are known about the scale of the loss but the German government published a report stating there was "massive damage to the plant".

In such events companies will be completely uninsured for these losses unless they have taken out a dedicated cyber policy with the appropriate coverage.

Cyber Incident – an incident can be considered an accidental cyber event such as a computer system failing to operate or operating incorrectly due to an error or omission by the insured.

Cyber Act – a cyber attack against either the insured or a third party, usually perpetrated by a bad actor, which leads to the insured sustaining damage.

Data coverage gaps

Coverage for the repair or replacement of damaged data remains broadly similar under the LMA5400 to the previous NMA2915. However, if an insured does not already have a standalone cyber policy they need to consider not just the replacement, but the recreation of data.

Shipping giant Maersk were famously hit by an attack known as NotPetya in 2017. The attack was actually targeting the Ukrainian software company, Linkos, but inadvertently hit around 2,000 companies worldwide, including Maersk. Within 7 minutes the entire worldwide operations of Maersk were brought to a standstill and almost all data, including back-ups, were totally wiped from their systems. In such an event there would be no back up data to replace or repair this lost data. An insured suffering an attack like this would need to recreate all their data and system architecture from scratch – something not included under property policies where any of these exclusions have been applied. The only way to get a company running again would be to recreate the data, which can be an extremely costly and time consuming way to get back online.

Furthermore, under the LMA5401 there is a full exclusion on data, which means no coverage will be provided even for the repair or replacement from any proximate cause – **including property perils**. Cyber policies will not cover data loss from property perils either and so this is an important area for clients to consider.

A standalone cyber policy is, however, the best way to ensure your data is covered following a cyber attack or operational error. Through such policies insureds can be confident their data is covered even if back-ups are destroyed.

Data Replacement – replacing data refers only to the costs of restoring data from back-ups. The process can be costly for large companies as multiple back-ups from many locations may be required to replace the lost data in full.

Data Recreation – when data cannot be replaced or restored because back-ups were not saved recently, or have been damaged, or simply do not exist then data must be recreated. In extreme cases this may mean manually retyping data, creating new code or copying paper files.

How can BMS help?

The cyber market is primed to help protect insureds from the coverage gaps these new exclusions are creating. There are three key forms of this: affirmative coverage, write-back policies and difference in conditions/difference is limits (DIC/DIL) cover.

Affirmative coverage

Modern cyber policies in the London market should cover the recreation of data from both cyber attacks and accidental cyber events. However, affirmative property damage coverage within the cyber market which explicitly provides indemnity for resultant damage is less common. In the past year, this market has grown as the market prepares for the influx of enquires following the use of these exclusions by non-cyber markets. The underwriting process can usually be conducted using the property submission and a short cyber application form and premiums are competitive given the current soft state of the cyber market. Affirmative coverage is however more expensive than a DIC/DIL policy, but provides greater peace of mind.

Write-back policies

Since the changes were introduced, some markets have started offering write-back policies. These aim to cover events which would be excluded, via one of the new exclusions applied to an insured's non-cyber policy. While these may seem like a great way to cover any gaps created by a new exclusion, the write-backs do not provide a perfect fit. They often come with their own embedded exclusions, usually excluding any event caused by a Cyber Incident (accident) and any coverage for data loss. These policies can sometimes be cheaper than the affirmative coverage options, but they also rely on the non-cyber policy first rejecting a claim before this one can trigger.

DIC/DIL

Some London cyber markets now provide a DIC/DIL property damage option within their cyber policies. This usually operates if the property policy denies a claim due to a cyber exclusion; the cyber policy will then drop down to cover the resulting loss. It also provides standalone cyber coverage which is primary and unrelated to the property policy – so your data is affirmatively covered. Ultimately this is a cheaper option than the affirmative coverage above but there are some limitations. Consider, for example, the time it may take to pay a claim if the property policy must first deny a claim. Nonetheless, having a DIC/DIL policy in place can ensure that some gaps in coverage created by the exclusions mentioned in this paper are more adequately addressed.

BMS has a dedicated Cyber & Technology team experienced in placing complex risk managed placements where coverage gap issues may be present. Our broking team has over two decades of combined experience and are frequently engaged to support other lines of business facing cyber exclusion issues. The team also includes an in-house cyber security consultant who assists insureds in accurately modelling their cyber exposure.

Contact us

For more information please contact your broker or a member of our dedicated Cyber insurance team:

Simon Meech
Cyber Insurance Broker
Mobile: +44 (0)774-746-0022
Email: simon.meech@bmsgroup.com

James Gordon
Managing Director – Cyber & Technology Division
Direct: +44 (0)207-480-0365
Email: james.gordon@bmsgroup.com