SILENT CYBER AND CRIME COVERAGE

Confusion or Clarity?

June 2020

Lloyd's syndicates are required to clarify their position on 'silent cyber' in crime coverages from 1 July 2020 – but evidence to date suggests there is little consistency between insurers as to what that means in practice. Policyholders and their brokers therefore need to take care to avoid overly broad exclusions being applied, and ensure that appropriate crime cover is maintained.

In July 2019, Lloyd's of London mandated that all policies underwritten by Lloyd's syndicates should provide clarity regarding cyber coverage by either excluding it, or providing affirmative coverage. The aim of this was to deal with what is known as "silent cyber" or "non-affirmative cyber" – potential coverage for cyber exposures within traditional property and liability insurance policies, where cyber coverage is neither explicitly excluded nor clearly included.

Those traditional policies were not created with cyber exposures in mind. Accordingly, there have developed elements of overlap and duplication between those policies and stand-alone, specialist cyber insurance policies. The extent of that overlap is often unclear and coverage may be ambiguous, resulting in increased risk of disputes arising between policyholders and insurers and cover not matching policyholder expectations. Lloyd's, insurers and regulators have become concerned that silent cyber may represent an unexpected risk to insurers' portfolios with large unintended aggregate cyber exposures, particularly in classes of business where the overlap is unintentional and not priced in – such as all-risks property coverage, which operates on the basis that all risks are covered unless expressly excluded.

This has in turn prompted Lloyd's to take action, requiring Lloyd's syndicates to provide that clarity and ensure they have a proper understanding of the cyber risk attaching to their portfolios. Company markets are also following suit. That is in part for consistency, given many also operate a Lloyd's syndicate, and in part driven by comments from regulators such as the Prudential Regulatory Authority (PRA) on the need to ensure clarity and reduce their silent cyber exposure.

The changes are being introduced in stages. The first tranche was effective from 1 January 2020, applying to all first party property damage policies. The second tranche, more importantly for present purposes, commences on 1 July 2020 and includes Bankers Blanket Bond / crime policies. The final phases, which will include professional indemnity and other liability policies, will commence on 1 January and 1 July 2021.

WHAT DOES THIS MEAN FOR CRIME COVER?

Excluding or affirming cyber cover sounds simple in theory, but in practice has proven to be more difficult. The key question, ultimately, is 'what is cyber risk'? The definition put forward by Lloyd's and the PRA is:

"Any risk where the losses are cyber-related, arising from either malicious acts (e.g. cyber-attack, infection of an IT system with malicious code) or non-malicious acts (e.g. loss of data, accidental acts or omissions) involving either tangible or intangible assets."

Whilst the examples of 'malicious acts' provided are straightforward, the concept is problematic when considered in the context of crime policies. The core cover provided by those policies is for direct financial loss, and associated costs, arising from malicious (and dishonest, fraudulent and/or criminal) acts. The majority of crime incidents now involve use of a computer system, so any broad silent cyber exclusion framed around "cyber-related malicious acts" will also likely remove a number of core 'traditional' crime coverages. To use an example, the exclusion would apply to stolen funds arising from employee infidelity, where that employee had obtained unauthorised access to the insured's systems and processed fraudulent payments to their own account. This is a core 'traditional' crime cover, and not something that would be expected to be considered 'silent cyber' or otherwise excluded.

Care needs to be taken, therefore, to ensure: (i) that key cover is not removed: (ii) that exclusions define cyber risk appropriately: and (iii) that the focus is on areas where there is true overlap with cyber policies. The core overlap is in respect of coverage for cyber extortion (ransomware) and for certain fees, such as data recovery costs – so rather than excluding any 'cyber-related' loss, exclusions should ideally be focusing on excluding those overlapping coverages only.

This ensures that policyholders are not left with an unintended (on their part) gap in coverage between their crime policy, and the cyber coverage which is generally available in the market. That is particularly important here, as cyber policies do not generally provide coverage for theft of funds and other direct financial loss suffered as the result of a cyber incident – so there is potential for a very significant uninsured exposure to arise.

WHAT IS THE POSITION OF INSURERS?

With 1 July 2020 rapidly approaching, the Lloyd's Market Association (LMA) (with which many insurers are involved and from which they often take their lead) released their proposed clause on 22 June 2020. The LMA has proposed:

(i) To provide affirmative cyber cover where electronic and computer crime coverage is expressly provided for in the relevant crime policy; and

(ii) To exclude cyber cover where a crime policy does not expressly contain computer crime coverage.

This is likely to be helpful to policyholders in the financial institutions space, the majority of which will hold crime policies including electronic and computer crime cover (and so will benefit from the affirmative language).

Where that is not the case, however, the specific exclusionary language proposed by the LMA seeks in broad terms:

(a) To exclude all loss directly or indirectly arising from Cyber Acts (unauthorised, malicious or criminal acts involving access to or use of a computer system) and Cyber Incidents (both errors and omissions involving access to or use of a computer system, as well as system failure events involving inability to access or use a computer system); and

(b) To expressly state that such exclusion does not apply to the extent that the loss results directly from a Dishonest Cyber Act – being malicious or criminal acts involving access to or use of a computer system.

We consider that as a broad approach this is likely to be acceptable to most policyholders. Crime cover is not generally intended to include cover for Cyber Incidents (E&O and system failure cover), which would normally fall under professional indemnity and/or cyber policies. Likewise, unauthorised access to systems which was not malicious or criminal is likely to be a question of negligence rather than criminal behaviour, and so fall outside the scope of standard crime coverages.

That said, care will need to be taken to ensure that the scope of Dishonest Cyber Act is aligned with the particular policy in question – for example, many will be triggered by fraudulent, as well as malicious or criminal acts. Brokers will also need to ensure that there is clarity on the cover for 'indirect' losses such as fees coverage, given that the Dishonest Cyber Act cover applies only to loss arising directly from such acts.

It remains to be seen to what extent insurers will necessarily follow the LMA's proposed approach, so exclusions may still be applied even where electronic and computer crime coverage currently exists. Exclusionary language is likely, therefore, to remain relevant. To the extent that insurers have put their head above the parapet, we have seen various approaches to date.

Some have taken an approach that broadly accords with our and policyholder expectations as to how the exclusion ought to be framed. This includes those that have been similar in approach to the LMA form, so excluded loss caused by a tightly drawn definition of 'cyber act' reflecting triggers under a cyber policy, but importantly not including any malicious or criminal acts using a computer system. Others have excluded only specific fees / losses that would be covered under a cyber policy.

Others, however, appear to have given much less consideration to the risks of a gap in cover or, if they have, are happy to put that risk on to policyholders. Examples we have seen have excluded all loss directly or indirectly connected to unauthorised access to a computer – so would certainly exclude all loss arising from the employee infidelity example above. Another example seeks to exclude all loss "*caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system*". This is not tied to any particular computer systems and, quite clearly, would operate to exclude a substantial portion of the fidelity, extortion and third party / electronic and computer crime cover provided under a financial institutions crime policy.

WHAT SHOULD YOU DO?

The approach by insurers above may change how cyber risks are covered – or not covered – under existing insurance programmes. It is to be hoped that the LMA's proposal will result in affirmative cover being provided for many financial institutions crime policies. However, that may not always be the case and if not, given the range of exclusions being put forward, policyholders will need to carefully review their current policies alongside their broker and examine with their broker any exclusion proposed by their insurers, to ensure that they are fully understood and not overly broad.

Even if appropriate exclusions are applied, there may be areas (such as cyber extortion cover and/or fees) for which crime coverage is no longer provided. In such cases, a standalone cyber policy may be the best solution to ensure coverage and fill gaps resulting from a silent cyber exclusion.

CONTACT DETAILS

Ed Brennan
T: +44 20 7648 7347
E: edward.brennan@howdengroup.com

Neil Warlow
T: +44 20 3808 2542
E: neil.warlow@howdengroup.com

Howden Asset Management
One Creechurch Place, London, EC3A 5AF

T +44 (0)20 7623 3806
F +44 (0)20 7623 3807
E info@howdengroup.com

www.howdenam.com

Part of the Hyperion Insurance Group