LLOYD'S

Market Bulletin

Ref: Y5381

Title	State backed cyber-attack exclusions
Purpose	To set out Lloyd's requirements for state backed cyber-attack exclusions in standalone cyber-attack policies
Type	Event
From	Tony Chaudhry Underwriting Director
Date	16 August 2022
Deadline	From 31 March 2023 at the inception or on renewal of each policy
Related links	

The market for coverage against cyber-attack losses has grown rapidly in recent years to become a significant class of business for insurers. Lloyd's underwriters have led the way in providing cover, offering a valued product to clients.

Lloyd's remains strongly supportive of the writing of cyber-attack cover but recognises also that cyber related business continues to be an evolving risk. If not managed properly it has the potential to expose the market to systemic risks that syndicates could struggle to manage. In particular, the ability of hostile actors to easily disseminate an attack, the ability for harmful code to spread, and the critical dependency that societies have on their IT infrastructure, including to operate physical assets, means that losses have the potential to greatly exceed what the insurance market is able to absorb.

For this reason, we have consistently emphasised that underwriters need to be clear in their wordings as to the cover they are providing. Starting from 2020, on a phased basis, we required that all policies specify whether cyber cover is provided by either including affirmative cover or by excluding (see Market Bulletin Y5258). The Prudential Regulation Authority has similarly set out its expectations on cyber business in its Cyber insurance underwriting risk (July 2017); Supervisory Statement 4/17.

Lloyd's is authorised under the Financial Services and Markets Act 2000

War exclusions and cyber-attack cover

More recently, exposure to cyber-attack losses has been an area of market focus in circumstances where the losses arise from attacks sponsored by sovereign states. We already set out our requirements for war risks in our 'Performance Management: Supplemental Requirements and Guidance'. Cyber-attack risks involving state actors, however, have additional features that require consideration. In particular, when writing cyber-attack risks, underwriters need to take account of the possibility that state backed attacks may occur outside of a war involving physical force. The damage that these attacks can cause and their ability to spread creates a similar systemic risk to insurers.

We recognise that many managing agents in the market are already including clauses in their policies specifically tailored to exclude cyber-attack exposure arising both from war and non-war, state backed cyber-attacks. We wish to ensure, however, that all syndicates writing in this class are doing so at an appropriate standard, with robust wordings. We consider the complexities that can arise from cyber-attack exposures in the context of war or non-war, state backed attacks means that underwriters should ensure that their wordings are legally reviewed to ensure they are sufficiently robust.

Requirement for exclusions in standalone cyber-attack policies

It is important that Lloyd's can have confidence that syndicates are managing their exposures to liabilities arising from war and state backed cyber-attacks. Robust wordings also provide the parties with clarity of cover, means that risks can be properly priced and reduces the risk of disputes.

We are therefore requiring that all standalone cyber-attack policies falling within risk codes CY and CZ must include, unless agreed by Lloyd's, a suitable clause excluding liability for losses arising from any state backed cyber-attack in accordance with the requirements set out below. This clause must be in addition to any war exclusion (which can form part of the same clause or be separate to it). At a minimum, the state backed cyber-attack exclusion must:

1. exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.

2. (subject to 3) exclude losses arising from state backed cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.

3. be clear as to whether cover excludes computer systems that are located outside any state which is affected in the manner outlined in 2(a) & (b) above, by the state backed cyber-attack.

4. set out a robust basis by which the parties agree on how any state backed cyber-attack will be attributed to one or more states.

5. ensure all key terms are clearly defined.

Further, given the complexities that can arise in drafting suitable exclusion clauses, managing agents must be able to show that these exclusions have been legally reviewed having regard to the interests of underwriters.

For the 2023 year of account business planning process, we will be discussing with managing agents the clauses that they will be agreeing for use in standalone cyber-attack policies. Managing agents will be expected to demonstrate that the clauses they will be adopting meet the requirements set out above. Where managing agents wish to diverge from the requirements set out in this guidance, they will need to provide a robust explanation for their approach and receive agreement from Lloyd's.

LMA model clauses

The LMA has already undertaken an extensive exercise in producing suitable model clauses addressing state backed cyber-attacks, issued as LMA21-043-PD. Lloyd's is satisfied that where any of the four model clauses is adopted, this will meet the requirements set out above. It is nevertheless for managing agents to decide on which clause they wish to adopt, provided they can demonstrate that the clause meets the requirements set out above (unless they receive a dispensation from Lloyd's).

Implementation and next steps

The requirements set out here take effect from 31 March 2023 at the inception or on renewal of each policy. There is no requirement to endorse existing, in force policies, unless the expiry date is more than 12 months from 31 March 2023. Managing agents will nevertheless wish to start at an early stage to determine their approach to adopting appropriate exclusion clauses (including obtaining any necessary legal review).

In implementing the requirements set out above, managing agents also need to have regard to the terms of their reinsurance programmes, to ensure they provide appropriate, back to back cover.

Lloyd's is continually looking at systemic exposures in the Market. We will continue to monitor exposures within the cyber exposed classes and communicate any concerns that require action.

Further information

If managing agents wish to discuss Lloyd's requirements further, they should contact their Syndicate Performance Manager.