LLOYD'S

MARKET BULLETIN

REF: Y4938

Title	Cyber-attack: managing catastrophe-risk and exposures
Purpose	To provide details of exposure-management principles for Cyber-Attack, and related returns that managing agents are required to submit to Lloyd's
Type	Event
From	Tom Bolt Director, Performance Management
Date	9 November 2015
Deadline	31 December 2015
Related links	Market Bulletin Y4842 - Cyber Risks & Exposures

Purpose

Further to Tom Bolt's letter to CEOs about Cyber-Attack in September 2015, Lloyd's now wishes to provide further information about the oversight framework for understanding and managing catastrophe-risk (or accumulation-risk) for this emerging market exposure.

Definition of Cyber-Attack

For present purposes, Lloyd's focus is on exposures arising from a **malicious electronic act** which for the purpose of this bulletin we label as 'cyber-attack'. Cyber-attack is therefore the proximate cause of loss, although the consequences may include property damage, bodily injury, financial loss or other forms of damage.

Background

The risks posed by cyber-attack present an opportunity for the insurance market. We are keen for Lloyd's underwriters to continue to take a lead as a market with proven expertise and an ability to innovate.

Lloyd's also wishes to ensure, however, that cyber-attack exposures are underwritten with appropriate controls in place, and that aggregate exposures are appropriately monitored.

On 9 September 2015, the Director of Performance Management sent a letter to the CEOs of all managing agents setting out principles for understanding potential cyber-attack losses across classes of business, and for monitoring aggregate exposures to cyber-attack.

This bulletin provides more detail on Lloyd's new requirements for cyber-attack, and describes the work that Lloyd's and the LMA are undertaking over the next few months.

We have also restated the requirements from the letter to CEOs so that all cyber-attack related activities are detailed in full. Appendix 1 contains a timeline of activity relating to cyber-attack.

Executive Summary

Oversight Framework for Cyber-Attack Exposure Monitoring

It is essential that syndicates' cyber-attack exposures are clearly understood and recorded so that Lloyd's can properly consider the market's accumulation-risk. Accordingly Lloyd's requires the following to be put in place to ensure that syndicates have a robust approach to the management of cyber-attack risks and exposures:

1. Lloyd's requires syndicates to have a specific risk-appetite for cyber-attack across all classes of business, signed off by their Boards, for all policies in force from 31 December 2015.

2. Structured processes for understanding cyber-attack exposures by class of business are to form part of syndicates' formal risk management frameworks. Managing agents must complete an initial review of cyber-attack exposures by 1 April 2016, and confirm to Lloyd's that that this has been done.

3. Syndicates are required to adopt a scenario-based approach for considering gross aggregate exposure to cyber-attack. Each syndicate must conceive and design at least three internal scenarios for this purpose. This is a minimum – the number and type of internal scenarios is otherwise entirely at syndicates' discretion. Having created the internal scenarios, syndicates must then estimate their aggregate potential exposures to each, across all affected lines of business and report aggregate exposures to Lloyd's by 1 April 2016.

Reporting Requirements

The following **reporting framework for cyber-attack** will apply:-

- submission of risk-appetite statements along with details for managing cyber-attack risk relative to risk appetite

- confirmation of the introduction of a cyber-attack exposure risk-management framework

- gross aggregates: details of the internal 'cyber-attack scenarios' which generate the three largest gross aggregate exposures; estimates of gross aggregate exposure for each scenario; and – at syndicates' discretion – the related scenario PMLs. Reporting should be both gross and net of reinsurance

Note: This cyber-attack exposure monitoring oversight framework is intended to address potential exposure on an aggregate basis and does not of itself affirm the existence or absence of coverage under any specific policy. Coverage is dependent on the facts of a specific claim at issue and the terms and conditions of the policy under which such claim is submitted.

LMA process

The LMA is consulting its underwriting Committees and Panels to gather information about cyber-attack scenarios that may arise across different classes and types of risk. This information will be provided to Lloyd's and Lloyd's will provide feedback on the LMA process to the market by 30 November 2015, enabling managing agents to consider the outputs as part of the oversight framework described in this Bulletin.

Delegated Authority business should be included in managing agents' cyber-attack exposure management processes by 1 October 2016. The LMA will run a second consultation with the members of its Delegated Authority Committees. They will review the consultation feedback, and the approach to gross aggregation monitoring detailed in this Bulletin. The Delegated Authority Committees' feedback will be provided by Lloyd's to managing agents by the end of the first quarter of 2016.

Timeline

A timeline of cyber-attack activity is provided with this Bulletin in Appendix 1 to ensure that managing agents are aware of Lloyd's, LMA and syndicate work and deadlines throughout the remainder of 2015 and 2016.

Detailed Oversight Framework for Cyber-Attack Exposure Monitoring

1. Cyber-attack risk appetite

Lloyd's requires all syndicates to have a specific risk appetite for exposure to cyber-attack across all classes of business, signed off by their Boards, for all policies in force from 31 December 2015.

Managing agents must also have defined processes for managing cyber-attack risk relative to risk appetite, also signed-off by their Board.

Syndicates will be required to submit to Lloyd's their risk appetite statements for cyber-attack risk including their processes for managing cyber-attack risk relative to risk appetite. These should be submitted to Exposure Management in Lloyd's PMD by 31 March 2016.

The managing agent's internal audit function must regularly review business as usual implementation of the processes, including quarterly Board reporting.

2. Cyber-attack risk management framework

Lloyd's wishes to ensure that managing agents have a clear understanding of the potential for cyber-attack losses under all policies, both insurance and reinsurance.

To facilitate this aim, Lloyd's requires all managing agents to build a regular review of cyber-attack exposures across all classes of business into their risk management framework. This review should document, for each class of business, where exposures potentially exist and the amount of limit potentially exposed.

The first review should be completed by 1 April 2016. Confirmation that managing agents have completed the review, and added the review process to their risk management frameworks, should be furnished to Lloyd's.

This work is viewed as a critical first step. All managing agents must have a clear understanding of cyber-attack exposures. It is expected that the regular quarterly returns detailed below (along with any more formal scenarios or RDSs that may follow) will use information in this review as a base for the submission.

3. Requirement to design and use 'cyber-attack scenarios' for calculating aggregate exposures

Lloyd's believes that the type and nature of a cyber-attack will dictate which classes of business may be exposed, and therefore the degree of aggregate exposure within syndicates. The diversity of the threat means that no one 'cyber-attack scenario' would necessarily meaningfully reflect all syndicates' aggregate exposures across the market at present.

Therefore, syndicates are required to design and create their own internal 'cyber-attack scenarios'.

Syndicates should consider what 'cyber-attack scenarios' would have the potential to cause material accumulation risk for their books of business, and create at least three such internal cyber-attack scenarios for the purpose of accumulation management.

For the present, Lloyd's will refer to 'cyber-attack scenarios' to distinguish this concept from formal, market scenarios such as RDSs.

3.1 Syndicate scenarios, rather than market-level

There are different types of cyber-attack, which could cause different types of harm: denial of service, data-theft, data-damage, reputational harm, physical damage etc. The economic damage for each type may differ, with consequences including direct financial loss, bodily injury or property damage.

Lloyd's believes that it is premature to create fully-defined scenarios, similar to the property catastrophe RDSs, with specified insured losses and types of exposure. Understanding of potential accumulation risk from cyber-attack, particularly for lines of business that do not explicitly address cyber-attack coverage, is at a much earlier stage[1].

Furthermore, Lloyd's strongly believes that gaining a plurality of views as to 'plausible but extreme' cyber-attack events is in itself extremely helpful at this stage in the evolution of the threat.

3.2 Creating 'cyber-attack' scenarios

Syndicates should create and develop their own lists of 'plausible but extreme' types of cyber-attack scenarios, with associated lines of business that may be affected. Affected policies to be considered should include specific cyber policies, 'incidental' cyber coverage granted (or limited or written back) in other policies, and policies which are altogether silent as to cyber-attack.

Each 'cyber-attack scenario' should have the following characteristics:-

[1] For this reason, the current Cyber RDS deliberately specifies only the broad nature of the event: syndicates individually decide the affected industry sector, and assume their ten largest clients in that sector are targeted. The results are not additive across syndicates. A similar approach is taken for the two Liability RDSs.

specific – the scenario should concern a particular type of cyber-attack, which should be a single event: note that multiple simultaneous attacks from a single point may be considered 'an event' for this purpose; targeted companies or sectors should be identified

relevant – the potentially insured consequences can be related to the syndicate's portfolio

measurable – the scenario enables reasonable consideration as to which classes of business may be exposed, and to what extent

recorded – the scenario, including assumptions about potentially insured loss and its derivation, is recorded in sufficient detail that a person with reasonable knowledge of the subject could understand it, and assess the syndicate's potential exposure to it

repeatable – the scenario must be capable of being re-run against in-force data in the future

representative – the scenario should be representative of similar exposures within the syndicate

plausible but extreme – the scenario should be of a severity that is similar to an RDS event, note that this applies to the event itself, rather than the aggregate exposure to the syndicate (i.e. a quite extreme *event* may not necessarily result in an extreme syndicate *exposure*)

Syndicates should consider a variety of cyber-attack scenarios. The materiality of each will vary considerably depending on the classes of business written by the syndicate.

The following recent government publication on cyber security and the role of insurance outlines as a minimum the types of risks and exposures that should be considered:

- UK cyber security: the role of insurance in managing and mitigating the risk:

  https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

  Additional examples of the consequences of specific cyber-attacks are contained in the following reports:

- Business Blackout; The insurance implications of a cyber attack on the US power grid:

  https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

- Sybil Logic Bomb Cyber Catastrophe Scenario

  http://cambridgeriskframework.com/getdocument/9

3.3 Calculating aggregate exposures

Having designed and created at least three internal 'cyber-attack scenarios', managing agents should estimate their potential aggregate exposure to each of them.

The purpose of the exercise is to understand the total possible aggregate exposure to single events.

The appropriate exposure to include in the gross aggregate return should be the largest possible loss on all policies affected by the scenario. This will vary by class of business and should follow existing methodology used by managing agents for aggregation monitoring, including in RDS returns.

Total possible exposure to each scenario should not take into account probability of occurrence or the distribution of potential severity at this stage.

Where for statutory, regulatory or practical reasons insurers cannot expressly exclude or specify the limits of potential coverage for losses arising directly or indirectly out of a cyber-attack, then for the sole purpose of conservative aggregation monitoring managing agents should treat all such policies as if the full policy limit were available to pay claims for loss from cyber-attack, without regard to whether or not individual policies would, in fact, respond to cyber-attack losses.

Reporting Requirements

1. Cyber-attack risk-appetite

Syndicates will be required to submit to Lloyd's their risk appetite statements for cyber-attack risk including their processes for managing cyber-attack risk relative to risk appetite. These should be submitted to Exposure Management in Lloyd's PMD by 31 March 2016.

2. Cyber-attack risk-management framework

The first review of potential cyber-attack exposures should be completed by 1 April 2016. Confirmation that managing agents have completed the review, and added the risk-management review process to their risk-management frameworks, should be furnished to Lloyd's along with the first quarterly aggregate exposure report, detailed in 3 below.

3. Requirement to design and use 'cyber-attack scenarios' for calculating aggregate exposures

Confirmation of the Board's engagement with the gross aggregate management processes detailed in this bulletin should be sent to Lloyd's PMD by the 1 January 2016.

Reporting should be made on a quarterly basis to Exposure Management in Lloyd's PMD.

The first report is required before 1 April 2016 for all policies in force on the 1 January 2016. Reporting will continue until further notice three months in arrears.

All reporting should be agreed and signed off by the managing agent's Board and should be provided for each of the 'Lloyd's 10'[2] classes of business.

For the purpose of reporting to Lloyd's, syndicates should submit the three internal scenarios to which they have the greatest aggregate exposures.

[2] 'Lloyd's 10' classes of business are: Accident & Health, Aviation, Casualty, Casualty Treaty, Energy, Marine, Overseas Motor, Property (D&F), Property Treaty & UK Motor

Reporting should contain a description of the cyber-attack scenario and any assumptions made when creating the scenario and calculating aggregations.

Returns should, at this stage, be completed on both a gross and net basis. To aid Lloyd's development of PML methodologies syndicates are encouraged to submit any additional consideration and calculations made when looking at the probable loss for their selected scenarios.

Appendix 1 cyber-attack reporting timeline details these requirements in chronological order.

Further work with the LMA

The LMA are running a consultation with their members and asking all of their underwriting Panels and Committees to evaluate the range of possible cyber-attack risks within their respective classes of business.

Lloyd's will collate the consultation responses and provide feedback to all managing agents by 30 November 2015.

This work will:

- Inform Lloyd's and support managing agents in their assessment of the relative risks of cyber-attack across classes of business which can be used in development of risk appetite setting, risk management frameworks and reviewing of returns
- Provide insight into underwriters' views on scenarios that could give rise to a cyber-attack loss. This will be used by Lloyd's in the development of PML guidance
- Provide further information on terms and conditions that address cyber-attack coverage by class
- Promote consideration and understanding of potential cyber-attack risks and exposures within each class of business

LMA Model Wordings

The LMA is currently assisting relevant underwriting Panels and Committees in the development of additional model clauses for use where there are cyber-attack risks.

PML Methodologies

Lloyd's PMD will work with the LMA to review possible loss scenarios across classes of business using the LMA consultation responses on cyber-attack risks and exposures as a base.

Suggestions as to possible loss scenarios methodologies will be provided to the market by end of the first quarter 2016. Any changes required to RDSs for 2017 business planning will be made by May 2016, although at this stage Lloyd's is not necessarily considering formal RDSs.

Delegated Authority Business

The treatment of exposures under binding authorities and other delegated authority business should follow the same principles for gross aggregation monitoring as open market placements. Nevertheless, given the nature of these arrangements Lloyd's recognises that more time may be required to understand exposures.

Managing agents should work to include these policies into their processes by the fourth quarter 2016 cyber-attack return.

The LMA will review the cyber-attack consultation feedback with the delegated authority panels, and Lloyd's will publish any additional feedback from these panels in the first quarter of 2016.

Franchise Guidelines

This cyber-attack data collection exercise and reporting is not included as part of Lloyd's formal RDS processes. As such it will not fall under the Franchise Guidelines for exposure management.

Risk Coding

Managing agents are reminded of the requirement to code cyber exposures to the appropriate risk codes CY and CZ. More detail can be found in Market Bulletin Y4842 issued in November 2014.

Capital

Managing agents should note that cyber-attack aggregation exposures have the potential to impact adversely on a syndicate's capital requirements.

Further Information

Any questions should be directed to your Syndicate Underwriting Performance executive in the first instance or otherwise contact the Class of Business team at: classofbusinessreview@lloyds.com.

Appendix 1: Cyber-attack reporting timeline