LLOYD'S

MARKET BULLETIN

REF: Y4842

Title	Cyber Risks & Exposures
Purpose	To set out changes to Lloyd's monitoring of Cyber risks, including a new definition for risk code CY and a new risk code CZ
Type	Event
From	Tom Bolt Director, Performance Management
Date	25 November 2014
Deadline	1 January 2015
Related links	www.lloyds.com/riskcodes

Following consultation with the market, Lloyd's is revising its approach to the monitoring of cyber risks. Managing agents are asked to note the following:

- The definition of risk code CY has been updated
- A new risk code CZ is being introduced
- The Exposure Management team will be reviewing Lloyd's approach to aggregation monitoring during 2015. As a first step, Lloyd's will be undertaking a data collection exercise to assess syndicates' aggregation of exposures

Background

As the internet, IT and operational technology have developed over the last 20 years, individuals and businesses have become connected to each other more frequently and in more advanced ways than ever before. This development has impacted how we all do business for the better. At the same time, this has had the consequence of increasing all industries' cyber exposure, leading to a dramatic escalation in levels of risk.

For the insurance industry, this is an area of new and rapidly growing risk where the Lloyd's market is showing innovation and bringing its specialist insurance expertise to bear. We are keen for Lloyd's underwriters to continue to take that lead.

However, while the underwriting of cyber risks provides opportunities for Lloyd's syndicates, Lloyd's is concerned that without proper controls there exists a material risk of a dangerous

aggregation of exposure in the market. Lloyd's is also concerned that cyber risk may not be being properly priced for nor the exposures adequately quantified by managing agents.

On 1 October 2014 the Performance Management Directorate (PMD) initiated a consultation exercise with the market, via the LMA, to gather thoughts on how cyber risks and exposures should be coded and managed. Lloyd's was pleased with the number and detailed nature of the responses received and wants to extend its thanks to those in the market who found time to provide their views.

Having considered the views of the market Lloyd's is introducing a limited number of changes to allow for better monitoring by managing agents and Lloyd's. These changes will allow for more targeted interventions, where required. Specifically, Lloyd's has created a new risk code CZ and is updating the definition of risk code CY. In addition, PMD will be reviewing syndicates' policies for monitoring cyber accumulations and loss-estimation, which should comply with the Minimum Standards for exposure-management. The Cyber Scenario data collection exercise will be re-run as part of the 2015 RDS.

Cyber exposure – scope

The changes Lloyd's is implementing are intended to allow better monitoring of cyber exposures which arise from a malicious electronic act which for the purpose of this bulletin we label as 'cyber-attack'. Cyber-attack is therefore the cause of loss but the consequences could be property damage, bodily injury or financial loss. These exposures are contained, to a greater or lesser extent, within all classes of business.

In the 1 October 2014 consultation, Lloyd's asked consultees if they agreed that Lloyd's should limit its focus to cyber-attack. A range of views was expressed but overall Lloyd's believes that there is a consensus that the primary area of focus should be cyber-attack. The area of cyber coverage is, however, one that is developing rapidly and Lloyd's will keep its approach under review.

Cyber risk codes – CY and CZ

In the 1 October 2014 consultation document we indicated our intention to update risk code CY. In addition, as a result of market feedback, Lloyd's is also introducing a new risk code CZ. These risk codes and their definitions are set out below:

CY – Cyber security data and privacy breach: Coverage in respect of first or third party costs, expenses or damages due to a breach (or threatened breach) of cyber security and/or privacy of data, that does not include damage to physical property

CZ – Cyber security property damage: Coverage in respect of first or third party costs, expenses or damages due to a breach of cyber security that includes damage to physical property

- Use of codes and Multiple Risks coding

The two codes should be used where underwriters are marketing a specific, stand-alone product to respond to cyber losses. Appendix 1 provides more detailed guidance on the use of the risk codes.

Where cyber-attack cover is given as an add-on or extension to an existing policy (including where cyber-attack exposure is given as a result of cover not being excluded), then this should continue to be coded according to the predominant parts of the total risk as long as the guidance on the coding of multiple risks is followed. See in particular paragraph 3.5.1 of 'Risk Codes, Guidance and Mappings' (November 2014), which provides:

> *3.5.1 For insurances providing coverage across two or more risk codes (including those denoting both risk and territorial exposure) and in particular large global policies, the leading underwriter should code the predominant parts of the total risk having regard to the overall exposure of risk and the most likely incidence of future claims. The leading underwriter should endeavour to sub-divide the exposure into more than one risk code if the exposure is considered material, and to provide an appropriate division of premium.*

Note that paragraph 3.5.1 applies to risks where the policy covers both risk codes CY and CZ (i.e. cyber-attack policies covering property damage and breach of privacy) as well as for policies that have both cyber-attack and non-cyber-attack coverage.

Underwriting, Exposure Management, Capital and Business Planning

Note: the following section applies to all cyber-attack exposures, whether coded CY, CZ or included within coverage provided under a different risk code (and coded as such in accordance with paragraph 3.5.1 of 'Risk Codes, Guidance and Mappings').

- Underwriting

As cyber exposure continues to be a developing area Lloyd's expects that managing agents will take particular care in the underwriting of cyber-attack risks. Managing agents should therefore have processes in place to ensure that cyber-attack exposures are considered in appropriate detail when underwriting and pricing risks. Terms and conditions should be contract certain and where underwriters are excluding cyber-attack it is important to ensure that the wording accurately reflects the underwriter's intentions.

- Exposure management and loss-estimation

Managing agents are required to manage exposure to cyber-attack in line with Lloyd's current Minimum Standards. This includes:

- recording, monitoring and reporting cyber exposure, howsoever assumed
- understanding total exposed cyber aggregate
- where appropriate, having a defined risk appetite for cyber
- having defined processes for loss-estimation – including scenario-based methods where appropriate – and understanding the materiality of potential losses within the context of the syndicate's overall business; such processes should take account of the uncertainty around origin and quantum of losses for cyber

Lloyd's will re-run the Cyber Scenario data-collection exercise that formed part of the 2014 RDS. This will be on the same basis as the 1 January 2014 return, meaning that managing agents should include losses from all risk-codes (not just CY) that they believe may have exposure to a cyber event. This will form part of the 2015 RDS return.

Following the data-collection exercise, during the first half of 2015 PMD will review the results of the exercise with the LMA and managing agents. PMD will also review syndicate management of cyber-attack exposures as part of Minimum Standards assurance work during 2015.

Lloyd's Emerging Risks team will continue to explore additional scenarios to represent other aspects of cyber accumulation risk.

- Capital

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

- Business Planning

While there will now be two cyber related risk codes, Lloyd's does not require managing agents to resubmit their business plans, which will continue to show all cyber business under the CY code. Managing agents should, however, record risks as they are written under the appropriate risk code, either CY or CZ. Where managing agents resubmit their business plan for any other reason then they should update their business plan at that time to show CY and CZ planned business separately.

- Atlas system - coverholder class of business permissions

All Coverholders who currently have Atlas permissions for 'Cyber Liability' will automatically be given permission for the new 'Cyber' class of business that is replacing 'Cyber Liability'. This will allow for both the CY and CZ risk code. Managing agents therefore do not need to take any further action.

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 – Detailed guidance on use of CY & CZ risk codes

	When should a coding be made to?	What are the typical features of products?
CY **Cyber security data and privacy breach**	- When a product is marketed specifically to provide cover for losses flowing from a malicious electronic act - Where physical property damage is not covered by the policy - Insurance or reinsurance transactions	- Privacy/data breach products (which would typically include hacking, malware, , unauthorised use or access to a network, or other breach of cyber security) - Costs and expenses including notification costs, credit file monitoring, regulatory defence costs, forensic costs - Cyber extortion - Cyber terrorism where the target is data or privacy related - Cyber crisis management, PR and reputation coverage - Denial of service attack, Business interruption or additional costs of working - Data restoration costs for damage to data caused by a malicious electronic act - Fines and penalties
CZ **Cyber security property damage**	- When a product is marketed specifically to provide cover for losses flowing from a malicious electronic act - Where physical property damage is covered by the policy - Insurance or reinsurance transactions	- Cyber-terrorism or cyber-attack cover - infill or gap policies to write back exclusions such as CL380 in any class of business - Business interruption or additional costs of working - Other first and third party cost, expenses or damages may be covered under the policy