BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Chris Moulder
Director, General Insurance
Prudential Regulation Authority
20 Moorgate, London, EC2R 6DA

14 November 2016

Dear CEO

CYBER UNDERWRITING RISK

In the past few years, cyber insurance has been a key growth area for insurance and reinsurance firms against a background of softening rates and challenging market conditions. The prudential risks emanating from this fast-evolving field, if not managed well, are potentially significant to the viability of the firms involved and the reputation of the UK insurance industry as a centre of excellence and innovation.

In order to assess these risks, the Prudential Regulation Authority (PRA) carried out thematic work involving a range of stakeholders including insurance and reinsurance firms, (re)insurance intermediaries, consultancies, catastrophe modelling vendors, cyber security and technology firms, and regulators. The meetings took place from October 2015 to June 2016.

The PRA's work focused on the underwriting risks emanating both from affirmative cyber insurance policies, but also from implicit cyber exposure within 'all risks' and other liability insurance policies that do not explicitly exclude cyber risk. This latter type of cyber risk is referred to as 'silent' cyber risk in this letter.

The results of this work are summarised below and have highlighted several challenges facing the insurance industry in relation to cyber underwriting risk.

Results

1. **'Silent' cyber risk is material**: The PRA's work found an almost universal acknowledgement of the loss potential of cyber exposures endemic in 'silent cyber'. However, most firms did not demonstrate robust methods for quantifying and managing 'silent' cyber risk.

2. **'Silent' cyber loss potential increases with time**: It is the PRA's view that the potential for a significant 'silent' cyber insurance loss is increasing with time. As both 'silent' cyber insurance awareness and the frequency of cyber-attacks grow, so does the loss potential from 'silent' cyber exposures. There was some recognition that insurance firms may find it increasingly challenging to argue that all risks or other liability policies did not intend to cover this type of risk given the publicity and awareness of the issue.

3. **Casualty (direct and facultative) lines potentially significantly exposed to 'silent' cyber**: Casualty lines are potentially significantly exposed to silent cyber losses. This is either due to the fact that exclusions are not widely used or because some policies cannot reasonably exclude cyber losses. An example of the latter is Directors and Officers (D&O) policies. There is wide acceptance in the market that these policies are potentially exposed and should therefore respond to cyber claims. This is due to the nature of the D&O products, covering the broad range of risks Directors and Officers are exposed to. The PRA's findings also suggest that professional indemnity (PI), financial institutions (FI) and general liability (GL) products are also likely to be exposed to various degrees to 'silent' risks due to a lack of use of effective exclusions.

4. **Potential for 'silent' losses in marine, aviation, transport (MAT) and property lines**: The PRA's thematic work showed that aviation underwriters are comfortable providing implicit cyber coverage (ie no exclusions are used currently) despite a background of continuous technological advances in aviation electronics, arguing that the risk is zero or minimal, which is concerning. The same holds true for motor despite the developments in autonomous vehicles and questions in relation to their cyber security. Property underwriters acknowledged the potential for cyber aggregation resulting for example from cyber attacks on high-profile commercial or industrial targets, or from smart-house technology. Despite that, there are currently no widespread exclusions for cyber risk and the thinking around how to price or manage this risk does not appear to the PRA to have developed sufficiently.

5. **The exposure and response of reinsurance contracts is uncertain**: The PRA's work showed that reinsurers are aware of the potential aggregations resulting from 'silent' cyber and are looking to address this in future contracts. Currently, there is no widespread use of exclusion in either property or casualty reinsurance contracts. The PRA's work has not clearly demonstrated that this element is actively priced in to reinsurance contracts or managed otherwise. The PRA's discussions with key stakeholders suggest that where wordings exist to address the issue, these are bespoke and were introduced only recently. Given these wordings are not universally accepted and untested in time they may result in disputes should a cyber claim arise.

6. **Most firms lack clear strategies and risk appetites**: The PRA's work has shown that firms do not currently have clear strategies and risk appetites for managing cyber risk both affirmative and 'silent'. Despite cyber insurance being a key area of growth and risk, boards do not own the overall strategy around cyber risk and in a number of cases a clear strategy, supported by risk appetite statements, does not exist. This includes, but is not limited to, defining target industries to focus on, managing 'silent' cyber risk, specifying rules for line sizes, aggregate limits for geographies and industries and splits between direct and reinsurance.

7. **Firm investment in developing cyber expertise is insufficient**: There is currently insufficient investment from firms in developing their internal knowledge and expertise on both the affirmative and 'silent' cyber risk elements. This is due to a combination of: a) the early stage of development of their cyber offering; and b) the lack of supply of skilled professionals with cyber underwriting expertise. The PRA's work has also identified that growth aspirations in affirmative cyber are seldom accompanied by a commensurate investment in underlying expertise and talent.

8. **Affirmative cover risks are not well understood**: The PRA's work suggests that firms do not understand sufficiently the aggregation and tail potential of affirmative cyber cover. The advent of the cloud and the continuous evolving nature of the cyber landscape create significant challenges that potentially are unique to this line of business. Firms are limited by a lack of expertise and an insufficient length of claims data. Moreover, using past claims data to estimate future cyber losses may not be appropriate due to data being non-stationary.

9. **Risk management's ability to challenge is limited**: Risk management teams are often not adequately equipped - in terms of skills and expertise - to provide effective challenge to the business. In most cases, risk management input is limited to either developing simple deterministic scenarios or reviewing and adapting widely publicised work on the topic. This is concerning given the continuously developing nature of cyber risk and the importance of risk management as the second line of defence.

10. **Third-party vendor models at early stages of development**: The main catastrophe modelling vendors have expressed their commitment to developing fully probabilistic cyber catastrophe models. However, development is at an early stage and it may take a few years before the first versions are available. Catastrophe modelling vendors have developed small sets of deterministic cyber scenarios to assist their clients in managing aggregation, and data schemas have been developed for categorising cyber exposures. Although these are helpful steps, it is the PRA's view that the market has much work to do before it can capture and manage cyber exposures effectively**.**

11. **EU Data Directive will increase affirmative cyber exposures**: The implementation of the new Data Protection Directive in 2018 will strengthen the European regulatory framework on personal data. So far, firms have expanded their affirmative cyber coverage portfolios mainly in the United States. However, the forthcoming introduction of the Directive has seen a number of firms looking to expand their offering to Europe as well. Any perceived geographic diversification benefits for insurers could be offset by an increase in cyber risk aggregation potential.

In light of the above conclusions, it is the PRA's view that action is required across the non-life sector to mitigate the risks identified. The PRA has published a consultation paper (CP) on cyber insurance underwriting risk (CP39/16 'Cyber insurance underwriting risk') setting out its proposed expectations in relation to the prudent management of cyber underwriting risk. The CP sets out the PRA's expectations in relation to three main areas: i) management of 'silent' cyber risk, ii) setting clear appetites and strategies owned by boards and iii) investing in cyber expertise.

The CP is relevant to all UK non-life insurance and reinsurance firms and groups within the scope of Solvency II including the Society of Lloyd's and managing agents ('Solvency II firms').

Yours sincerely