BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Anna Sweeney
Director, Insurance Supervision

Chief Executives of specialist general insurance firms
regulated by the PRA

30 January 2019

Dear CEO

Cyber underwriting risk: follow-up survey results

In July 2017 we published Supervisory Statement (SS) 4/17 'Cyber insurance underwriting risk'.[1] This set out our expectations for insurers on the prudent management of cyber underwriting risk in three broad areas: i) actively managing non-affirmative ('silent') cyber risk;[2] ii) setting clearly defined cyber strategies and risk appetites that are agreed by the board; and iii) building and continuously developing insurers' cyber expertise.

In May 2018, and after discussing with industry associations and Lloyd's, we carried out a follow-up survey[3] involving firms of varying size. This letter provides feedback on the key themes that emerged from firms' responses, and areas where we think that firms can do more to ensure the prudent management of cyber risk exposures.

High-level thematic findings and future steps

The survey results suggest that although some work has been done, more ground needs to be covered by firms especially in relation to non-affirmative cyber risk management, risk appetite and strategy. Having reviewed firm's responses we also remain of the view that the expectations set out in SS4/17 are relevant and valid. Further details are provided below.

Non-affirmative cyber risk

1. Firms almost all agreed that a number of traditional lines of business have considerable exposure to non-affirmative cyber risk. Casualty, financial, motor and A&H lines were noted to have the largest non-affirmative exposure. Firms were also aligned in their view of low non-affirmative exposure for energy lines of business, mainly due to the application of exclusion CL380, a widely-used exclusion across marine lines.

2. There was significant divergence in firms' views of the potential exposure within Property, Marine, Aviation and Transport (MAT), and Miscellaneous[4] lines. Firms estimated their exposure to non-affirmative cyber risk on these lines to be anywhere between zero and the full limits. Some of the variation between firms may be explained by differences in the underlying portfolios and the extent to which firms have felt able to introduce sufficiently robust exclusions and/or limits. However, much of the divergence is likely to be reflective of differences in firms' perception of risk. This suggests that some firms should give further thought to the potential for cyber exposure within these specific portfolios.

3. Firms' quantitative assessments of non-affirmative risk are not well-developed and mostly rely on stress scenarios and expert elicitation. Firms with the most developed approaches had conducted detailed analyses and established processes for capturing cyber exposures for all products by bringing together different parts of the organisation (eg underwriting, risk, claims, IT, actuarial). This often included reviews of policy wordings and of the robustness of exclusions. The range of practices

[1] https://www.bankofengland.co.uk/prudential-regulation/publication/2017/cyber-insurance-underwriting-risk-ss.

[2] Defined in SS4/17 as 'insurance policies that do not explicitly include or exclude coverage for cyber risk'.

[3] See Annex, available at: https://www.bankofengland.co.uk/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results.

[4] This includes lines such as income protection, pet, travel breakdown assistance, legal expenses, fine art etc.

observed suggests that some firms should do more to carry out detailed assessments of their books of business and to develop means of more accurately assessing non-affirmative exposure.

4. Firms' stress test results suggest that a cyber event could have widespread impact on a number of different lines of business. Some firms assessed the potential risk of loss from cyber events as being comparable with major natural catastrophes in the US. This reinforces our concerns about the large exposure potential and the need for firms to take action to manage the unintended exposure to non-affirmative cyber risk.

5. Most firms expressed confidence in relation to the response of reinsurance programmes in the case of a large non-affirmative cyber catastrophe. However, the optimism expressed was not always corroborated by sufficient evidence. Some firms in our sample had examined the issue more closely and raised some concerns in relation to the potential coverage provided by reinsurers in comparison to firms' potential exposures. This was especially true in the case of excess of loss and other non-proportional reinsurance arrangements.

6. Firms noted limitations in the ability of their claims functions to distinguish and escalate non-affirmative cyber claims. This was typically due to a combination of lack of claims expertise and inflexibility of the claims process. This suggests that firms should review their claims processes to ensure they are fit for purpose in this area.

Affirmative cyber risk[5]

7. Survey results and further market intelligence point to a material widening of coverage for cyber insurance products. Three particular examples highlighted include coverage for business interruption (BI), contingent business interruption (CBI), and reputational damage. While broader coverage has clear benefits for policyholders and the wider economy, it also comes with obvious prudential risks for insurers if it is not accompanied by appropriate pricing adjustments and adequate risk management. This is particularly relevant given the relative lack of available data and immaturity of the cyber market compared to more established risk areas.

8. Firms' submissions of cyber stress tests (excluding non-affirmative cyber) suggested that gross losses could run in the multiples of annual cyber premiums. There was also significant divergence on the resulting losses among firms. This underlines the large uncertainty in cyber, the lack of reliable claims data and the immaturity of available models with potential links to capital adequacy.

9. In some cases, cyber limits are significant considering the relatively low premium volume and lack of comprehensive claims experience. This creates the potential for high volatility and reputational damage/private losses in the event of a significant cyber loss.

10. We will look to further understand some of these issues via an exploratory cyber stress test: the PRA's 2019 General Insurance Stress Test. The PRA intends to publish more details on its insurance stress testing plans for 2019 later this year.

Risk appetite and strategy

11. Firms acknowledged the necessity of having formalised risk appetites and a board-agreed strategy for both affirmative and non-affirmative cyber risk. However, survey responses indicate that progress has been varied and work has, in the main, appeared to focus primarily on affirmative cyber risk.

12. Firms reported that they were utilising Lloyd's and other available cyber scenarios along with catastrophe cyber risk models to inform their risk appetites. There was also an appreciation that the models are in their infancy and that their outputs should be reviewed against internally developed metrics. Firms with the most developed approaches had created bespoke scenarios which, they believe, better reflect their own underlying exposure.

[5] Defined in SS4/17 as 'insurance policies that explicitly include coverage for cyber risk'.

13. Most firms have made some progress on developing management information (MI) for the board. However, this mainly focuses on affirmative cyber risk by comparing exposure against scenarios and risk appetites. We have seen limited evidence for board MI on non-affirmative cyber risk. We believe there is scope for firms to make greater progress against this expectation.

Cyber expertise

14. Firms recognised the need to develop their knowledge further, due to the unique and evolving nature of cyber risk. In achieving this, firms acknowledged the input which can be provided by the Chief Information Security Officer or other existing technology expertise in the firm.

15. Firms make use of external expertise (catastrophe modelling vendors, consultants, legal advisors for wording assessments etc) alongside developing bespoke training programmes for board members and underwriters. A small number of firms have created internal 'centres of excellence' that enhance dissemination of cyber knowledge and risk management.

Next steps

Since the publication of SS4/17 we have engaged with several regulatory authorities and international forums to develop a co-ordinated approach in this field. This was in response to feedback we received from the insurance industry. We have been encouraged by the level of interest and engagement shown from the wider insurance industry and fellow regulators and continue to engage closely as we design and implement next steps.

Firms reported challenging market conditions, broker pressure, and lack of historic data, models, and expertise as the main impediments for the prudential management of cyber underwriting risk. We appreciate these challenges but do not believe they are insurmountable. We also welcome recent announcements about individual firms' efforts to manage non-affirmative cyber risk in their books of business.

The responsibility is on firms to progress their work and fully align with the expectations set out in SS4/17. In relation to the expectation that firms reduce the unintended exposure to non-affirmative cyber risk, insurers should develop an action plan by H1 2019 with clear milestones and dates by which action will be taken. Supervisors may ask to review this plan and subsequent progress towards it.

Over the rest of the year we plan to undertake the following steps:

- Provide further, targeted feedback to surveyed firms. We intend to arrange meetings with individual surveyed firms by the end of Q1 2019.
- Coordinate with Lloyd's to agree any follow-up actions in relation to Lloyd's managing agents.
- Carry out sample deep-dive reviews to other firms (not necessarily those in our initial sample) in H2 2019 to assess how these firms are meeting the expectations set out in SS4/17.

We will continue to keep this subject under review in the light of the progress firms make on these outstanding areas. Depending on progress, we will consider whether any further steps are appropriate in due course, such as potential revisions or additions to SS4/17.

Yours sincerely