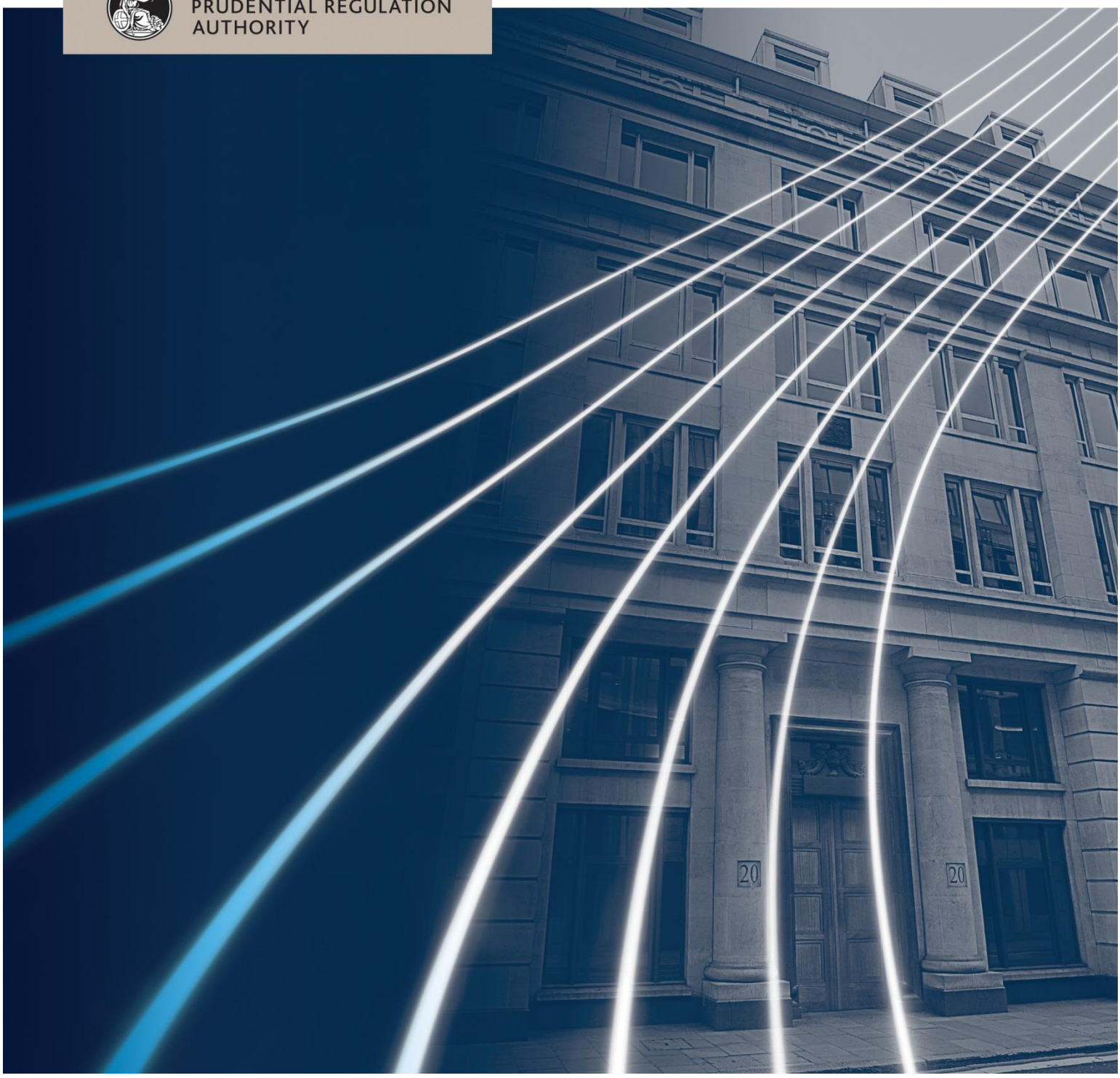
Policy Statement | PS15/17

Cyber insurance underwriting risk

July 2017

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY



Prudential Regulation Authority
20 Moorgate
London EC2R 6DA

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Policy Statement | PS15/17

Cyber insurance underwriting risk

July 2017

Contents

1	Overview	5
2	Feedback to responses	5
Appendices		8

1 Overview

1.1 This Prudential Regulation Authority (PRA) policy statement (PS) provides feedback to responses to Consultation Paper (CP) 39/16 'Cyber insurance underwriting risk' (the CP).[1] The PS also includes Supervisory Statement (SS) 4/17 'Cyber insurance underwriting risk', which sets out the PRA's final expectations regarding the prudent management of cyber insurance underwriting risk (see Appendix).

1.2 This PS 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').

1.3 Following consultation, there have been no material changes to the proposals. However, the PRA has made some amendments to the SS following various responses, in order to clarify. These are set out in Chapter 2. The PRA does not consider the changes to the consultation proposals to be significant and thus do not give rise to significant costs for firms.

2 Feedback to responses

2.1 The PRA is required by the Financial Services and Markets Act 2000 (FMSA) to consider representations that are made to it when consulting on its general policies and practices and its response to them.[2] This chapter sets out feedback to responses received to the CP.

2.2 The PRA received thirteen responses to the CP. Respondents were largely supportive of the proposals. The response to the feedback has been grouped by topic below.

Definition of 'cyber insurance underwriting risk'

2.3 Three respondents highlighted that the definition of 'cyber insurance underwriting risk' was not wide enough to include losses that emanate from sources other than a cyber attack and/or are not explicitly motivated to cause harm. These can include, but are not limited to, 'cyber errors', 'accidental loss of data' and 'use of Information Technology (IT) failures that result in physical damage to infrastructure and/or business interruption losses'.

2.4 The PRA has considered these comments and has further clarified the definition to explicitly include all potential sources of loss – both malicious and non-malicious – to which an insurance contract is potentially exposed.

Definition of 'silent' cyber risk

2.5 Four respondents pointed out that the use of the term 'silent' cyber risk is problematic and may create ambiguity in future arbitration or litigation cases. Two respondents suggested that the term 'non-affirmative' cyber risk should be used instead whereas one respondent suggested a distinction based on whether cyber-attack is a named peril or not. Finally, one respondent suggested that the distinction between 'silent' and 'affirmative' should be completely removed and instead referred to 'cyber risk exposures'.

2.6 The PRA's thematic review provided strong evidence of 'silent' cyber risk being a term that is widely understood and used by insurance professionals. However, the PRA agrees that the use of 'non-affirmative' cyber risk may be less ambiguous. We have amended the text of the SS reflect a distinction between: a) affirmative cyber risk (insurance policies that explicitly include coverage for cyber risk); and b) non-affirmative cyber risk (policies that do not explicitly

1 November 2016: www.bankofengland.co.uk/pra/Pages/publications/cp/2016/cp3916.aspx.
2 Sections 2N and 2L, FSMA.

include or exclude coverage for cyber risk). For completeness, the SS also notes that 'non-affirmative' cyber risk is often referred to as 'silent' cyber risk.

Line of business applicability

2.7 Two respondents questioned whether it was the PRA's intention to provide an exhaustive list of lines of business to which non-affirmative cyber risk applies. The PRA believes this is in relation to paragraph 2.5 of the CP where specific mention was made of casualty (direct and facultative), marine, aviation and transport (MAT) lines being "potentially significantly exposed to 'silent' cyber losses". These were provided in the CP only as examples for which the PRA believes that non-affirmative cyber risk may be material. However, the PRA's intention is for firms to have a broad scope when assessing and managing non-affirmative cyber risk. Therefore, the draft SS did not include an exhaustive list of specific lines of business. However, the PRA recognises that the SS may benefit from clarifying that the scope includes, but is not limited to, all Property & Casualty (P&C) covers and has amended the SS accordingly.

2.8 One respondent suggested that marine cyber risks should not be grouped with aviation and other transport lines in terms of potential levels of cyber losses. This was due to the low level of automation in the marine sector compared with aviation and transport. As noted above, both the draft SS and SS4/17 do not make reference to specific lines of business. Moreover, the PRA's thematic review did not produce convincing evidence to suggest that the marine sector is not in risk from material cyber losses. Therefore, no changes have been made to the SS.

List of potential actions for managing 'silent' cyber risk

2.9 There were a number of comments received in relation to the list of potential actions a firm could take to "actively manage their insurance products in relation to 'silent' risk exposures" provided in paragraph 2.2 of the draft SS. Most of these comments related to the suggested list of management actions being too prescriptive.

2.10 The draft SS explicitly mentioned in paragraph 2.2 that "firms could consider any of the following (the list is not exhaustive)". The PRA considers this is sufficient in re-assuring firms that it would consider any other actions that achieved the same purpose. However, the PRA has carefully considered these comments and has amended the SS to avoid any perception of being overly prescriptive.

2.11 One respondent was supportive of the recommendations and provided additional evidence that backed the PRA proposals in relation to 'silent' cyber risk. The respondent suggested that the PRA should strengthen the wording in the SS. The PRA has considered the comment but believes that the expectations set out in the SS are sufficiently robust. No change has been made as a result.

Strategy and Board Management Information

2.12 Three respondents raised concerns about the potentially prescriptive nature of the expectations set out in sections 3.2 and 3.3 of the draft SS which covers the risk appetite of the board. The PRA has carefully considered these comments and has taken some steps to alleviate any such perception. The examples in paragraph 3.2 of the draft SS are suggestions and firms could consider suitable alternatives. The amended text in the SS clarifies this further. The items listed in section 3.3 of the SS set out the PRA's minimum expectations that will enable boards to own and manage both affirmative and non-affirmative cyber risk. The PRA's thematic review findings have suggested that many boards have so far failed to proactively manage this risk. The requirement to confirm that current levels of premium are sufficient to

cover claims was removed based on feedback that it would be difficult to implement and may give the impression of being overly prescriptive.

2.13 One respondent raised a concern that the draft SS assumes that cyber risk is always material. Given the PRA's discussions with the thematic review participants, this is indeed the PRA's starting position. This is due to the endemic nature of non-affirmative cyber risk to potentially all P&C insurance contracts and/or the aggressive growth in affirmative cyber insurance. The above factors, combined with the explosive growth of the number of devices connected to a network suggest that cyber insurance underwriting risk will, in all likelihood, be a material risk for insurance firms falling within the scope of SS4/17. In relation to non-affirmative risk, where some ambiguity of the materiality of the risk may exist, the SS has been updated with the expectation that firms adopt a proportionate approach in assessing this risk. The PRA will however consider the specific risk for each firm in the context of its own business model.

2.14 Two respondents noted that the example of quantitative measures of aggregate geographical limits, provided in paragraph 3.2 of the draft SS, may not be as useful in relation to cyber risk. The PRA believes that there are instances where geographical concentrations may be a meaningful metric for assessing cyber exposures. However, the PRA acknowledges the concern given the non-geographic dependency of cyber threats. To avoid any confusion the specific example was removed in the SS.

2.15 Two respondents commented on the frequency of the management information (MI) to be signed-off by the board, noting that although affirmative cyber risk should be monitored on a more frequent basis, it would be impractical for most firms to review their non-affirmative exposures more than annually. The PRA agrees with the comment and has amended the text of the SS to clarify the frequency of reviews for affirmative and non-affirmative cyber risk.

2.16 One respondent raised concerns with regard to the limited availability of occurrence-based cyber policies and the ability of insurers to respond to an increased volume of cyber-related claims. The PRA notes the concerns but does not consider that the issues fall within the scope of the SS. No change has been made as a result.

2.17 One respondent argued that the draft SS was not consistent with the various regulations and guidelines mentioned in section 1.4. The PRA does not agree that the text goes beyond what is set out in the Directive, Commission Delegated Regulation and Guidelines, and the PRA approach document.[1] For risk management approaches to be adequate these expectations provide helpful guidance of some of the minimum requirements that these texts envisage. Particularly in the area of less known risks such as cyber insurance underwriting risk, examples are helpful for those firms that are less knowledgeable in these areas. It also reminds firms to ensure that they have considered all the elements, and none are overlooked.

Stress test return period

2.18 Some respondents pointed to the limited availability of historical data to support the calibration of extreme stress tests scenarios (up to 1 in 200 years) discussed in section 3.3 of the draft SS. It was suggested that the return period of such scenarios is reduced. The PRA has carefully considered the comments, and whilst it is appreciated that the availability of data is still developing, the PRA disagrees with the suggestion. Insurers should be able to quantify the risks they are exposed to and robustly capitalise against. As such, no change has been made to the SS.

1 March 2016: www.bankofengland.co.uk/publications/Pages/other/pra/supervisoryapproach.aspx.

Appendix

1 **Supervisory Statement 4/17 'Cyber Insurance Underwriting Risk', available at: www.bankofengland.co.uk/pra/Pages/publications/ss/2017/ss417.aspx**