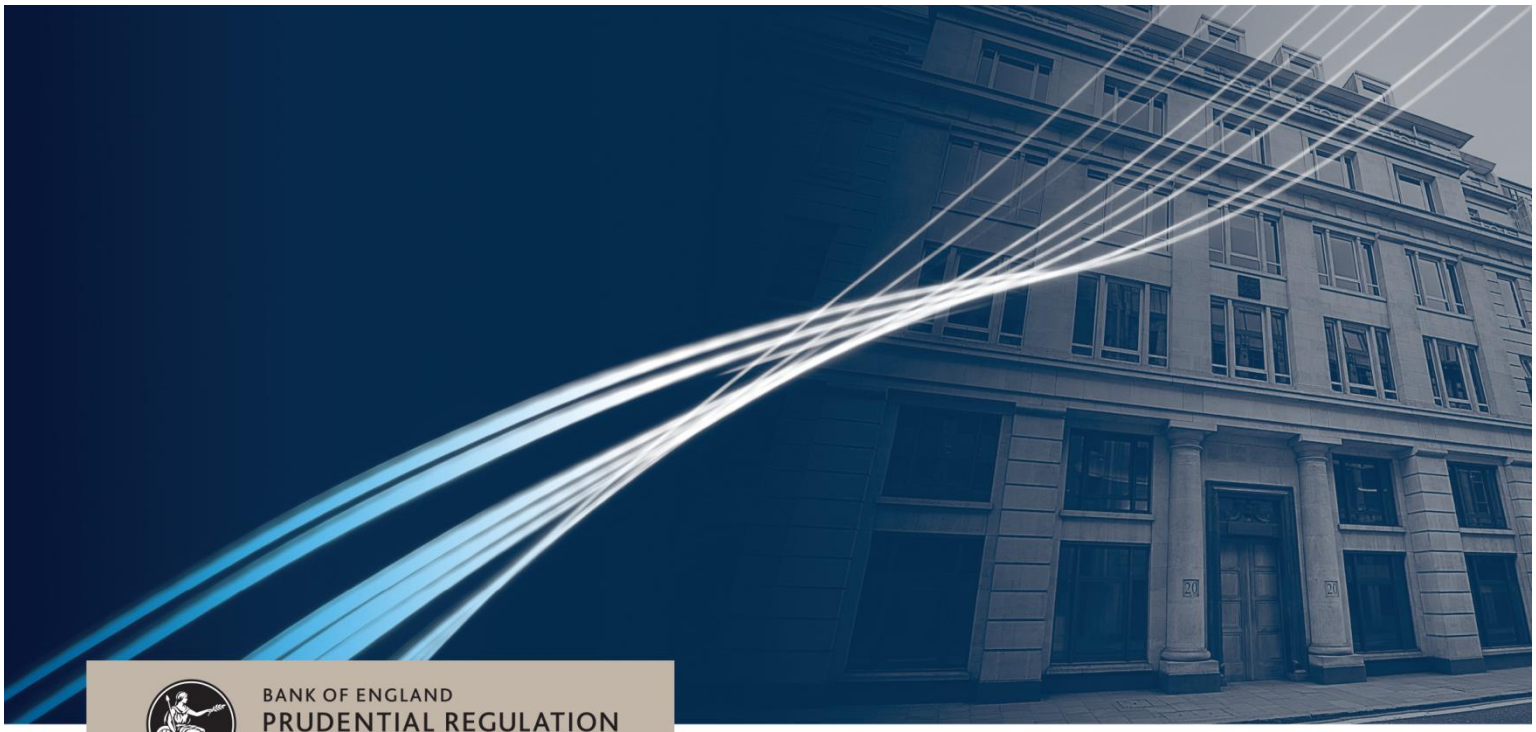

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Consultation Paper | CP39/16

Cyber insurance underwriting risk

November 2016

Prudential Regulation Authority
20 Moorgate
London EC2R 6DA

Prudential Regulation Authority, registered office: 8 Lothbury, London EC2R 7HH.
Registered in England and Wales No: 07854923

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Consultation Paper | CP39/16

Cyber insurance underwriting risk

November 2016

The Bank of England and the Prudential Regulation Authority (PRA) reserve the right to publish any information which it may receive as part of this consultation.

Information provided in response to this consultation, including personal information, may be subject to publication or release to other parties or to disclosure, in accordance with access to information regimes under the Freedom of Information Act 2000 or the Data Protection Act 1998 or otherwise as required by law or in discharge of the PRA's statutory functions.

Please indicate if you regard all, or some of, the information you provide as confidential. If the Bank of England or the PRA receives a request for disclosure of this information, the Bank of England or the PRA will take your indication(s) into account, but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on the Bank of England and the PRA.

Responses are requested by Tuesday 14 February 2017.

Please address any comments or enquiries to:
Alex Ntelekos
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

Email: CP39_16@bankofengland.co.uk

Contents

1	Overview	5
2	Proposals	6
3	The PRA's statutory obligations	7
Appendix: Draft Supervisory Statement 'Cyber insurance underwriting risk'		10

1 Overview

1.1 In this consultation paper (CP), the Prudential Regulation Authority (PRA) proposes a new supervisory statement (SS) setting out its expectations for the prudent management of cyber underwriting risk. For the purposes of the CP and draft SS, cyber underwriting risk is defined as the set of prudential risks emanating from underwriting insurance contracts that are exposed to losses resulting from a cyber-attack.

1.2 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').

Background

1.3 The proposals in this CP are based on thematic work carried out by the PRA between October 2015 and June 2016 involving a range of stakeholders including insurance and reinsurance firms, (re)insurance intermediaries, consultancies, catastrophe modelling vendors, cyber security and technology firms, and regulators.

1.4 The work focused on the underwriting risks emanating both from affirmative cyber insurance policies (eg data breach products), 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 CP.

1.5 The discussions with firms covered an array of relevant topics including:

- cyber underwriting strategy;
- target industries and product offerings;
- premium volumes, limits and line sizes;
- exposure management and reinsurance;
- 'silent' cyber exposure;
- risk management; and
- future of cyber offering/market.

1.6 The PRA also considered the views of insurance firms that had contemplated underwriting cyber insurance products but had decided that the uncertainty associated with the activity did not fit with their desired risk profile. In most cases firms were represented by their Chief Underwriting Officer, Chief Risk Officer, Chief Actuary, Lead Cyber Underwriter and Head of Exposure Management.

1.7 Discussions with other regulatory authorities focused on understanding the regulatory activity and awareness in other key markets.

1.8 When meeting with insurance intermediaries, technology firms, vendors of catastrophe models and cyber security firms, the PRA sought to understand the current status of products and services available to the insurance industry and the perceived needs of insurance buyers.

1.9 The results of this work highlighted several challenges facing the insurance industry in relation to cyber underwriting risk, which the PRA seeks to mitigate by the proposed expectations in relation to the management of both affirmative as well as 'silent' cyber risk set out in the draft SS in the appendix to this CP.

Next steps

1.10 This consultation closes on Tuesday 14 February 2017. The PRA invites feedback on the proposals set out in this consultation. Please address any comments or enquiries to CP39_16@bankofengland.co.uk.

2 Proposals

2.1 This chapter sets out the PRA's proposed expectations in relation to the ability of firms to exercise prudent management of cyber insurance underwriting risk. Firms are expected to be able to identify, quantify and manage the risks emanating from underwriting cyber insurance both in terms of affirmative and 'silent' cover.

2.2 The results of the PRA's work highlighted several risks faced by the insurance industry in relation to cyber underwriting risk. The key findings are summarised in a letter to firms published on 14 November 2016.[1]

2.3 The proposals have been grouped based on the PRA's thematic findings in the following sections:

- 'silent' cyber risk;
- cyber risk strategy and risk appetite; and
- cyber expertise.

2.4 The relevant chapters of the draft SS are noted below.

'Silent' cyber risk

2.5 The PRA has significant concerns about the loss potential of 'silent' cyber risk and has identified material shortcomings in the management of this risk. The conclusions drawn from the PRA's thematic work are:

- an almost universal acknowledgement of the loss potential of 'silent' cyber risk;
- that the potential for a significant 'silent' cyber insurance loss is increasing with time;
- that casualty (direct and facultative), marine, aviation and transport (MAT) lines of business are potentially significantly exposed to 'silent' cyber losses; and
- that the exposure and response of reinsurance contracts to 'silent' cyber risk is uncertain.

2.6 The PRA proposes that firms have the ability to monitor, manage and mitigate 'silent' cyber risk effectively, and aim to provide policyholders with greater contract certainty as to their level and type of coverage. The PRA's proposed expectations are set out in Chapter 2 of the draft SS.

Cyber risk strategy and risk appetite

2.7 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

1 'Cyber underwriting risk', www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf.

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.

2.8 The PRA proposes that firms exposed to 'silent' and affirmative cyber risk will have clear strategies and articulated risk appetites on the management of the associated risks. These should be owned by the board, and reviewed on a regular basis. The PRA's proposed expectations are set out in Chapter 3 of the draft SS.

Cyber expertise

2.9 The thematic work showed that 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.

2.10 The PRA proposes that firms have sufficient expertise to monitor and manage the risks emanating from cyber risk. The PRA's proposed expectations are set out in Chapter 4 of the draft SS.

3 The PRA's statutory obligations

3.1 When consulting on its general policies and practices, the PRA must fulfil several statutory and public law obligations, as set out in this chapter.

Cost benefit analysis

3.2 The proposals set out in this CP are designed to address risks related to cyber insurance underwriting that the PRA has identified following extensive thematic work with key stakeholders. The PRA's work suggests that most firms are not adequately equipped to monitor, manage and mitigate this risk. Current practice may also lead to policyholders not having the required contract certainty.

3.3 There will be some cost to the firms for implementing these proposals. The costs can be split in two parts, namely for addressing: i) 'silent'; and ii) affirmative cyber risk. The costs of addressing 'silent' cyber risk should be relatively uniform for all firms that are requested to increase their internal expertise in relation to this risk. However, a sub-element of the cost may depend on the nature of the portfolio and the mitigation techniques that the firm decides to put in place. For example, the cost associated with developing pricing models for 'silent' cyber risk may be different from applying exclusions or policy limits. The costs relating to affirmative cyber cover should be proportionate to the size of the cyber book but should take into account future growth targets in this space.

3.4 There are significant benefits to policyholders and to the resilience and reputation of the UK insurance industry should these proposals be implemented. The thematic work results suggested that cyber risk is material and could lead to potentially significant insured losses that extend beyond affirmative cyber cover and into traditional property and casualty (P&C) policies. By streamlining the approach that firms take in managing cyber risk the PRA will potentially limit the downside risk to the industry, from both the point of view of capital stress, and in terms of protecting the reputation of the UK insurance industry. Moreover, the implementation of the proposals will lead to increased contract certainty for policyholders of

traditional P&C policies who under the current regime may find it challenging to understand whether they are covered for this risk.

3.5 Based on the analysis above, it is the PRA's view that the benefits from the implementation of these proposals far outweigh the associated costs.

Compatibility with the PRA's objectives

3.6 In discharging its general functions, the PRA must, so far as is reasonably possible, act in a way which advances its general objective of promoting the safety and soundness of PRA-authorised persons[1], and in relation to insurance, which is compatible with its insurance objective of contributing to the securing of an appropriate degree of protection for those who are or may become policyholders.[2] The PRA must also have regard to the need to minimise any adverse effect on competition in the relevant markets that may result from the manner in which the PRA discharges those functions.[3]

3.7 The proposals are intended to give policyholders greater confidence in terms of insurers' contractual obligations around the coverage of cyber risk. Prudent management of all elements of cyber risks enhances the safety and soundness of firms and in the long term secures an appropriate degree of protection for policyholders.

3.8 The PRA has assessed whether the proposals in this CP facilitate effective competition. The proposals in this CP are expected to contribute to greater market discipline around the management of cyber risk, which should promote effective competition.[4]

Regulatory principles

3.9 In discharging its general functions, the PRA must also have regard to the regulatory principles as set out in section 3B of the Financial Services and Markets Act 2000 (FSMA).[5] Three of the principles are of particular relevance:

- that a burden or restriction which is imposed on a person, or on the carrying on an activity, should be proportionate to the benefits, considered in general terms, which are expected to result from the imposition of that burden or restriction. The PRA has followed this principle by issuing guidance on the management of cyber underwriting risk that balances the prudential risks emanating from this activity to the relative growth aspirations and the overall exposure assessment of firms to cyber risk;

- the responsibilities of the senior management of firms subject to requirements imposed by or under this Act, including those affecting consumers, in relation to compliance with those requirements. By setting proposals that link the assessment and management of cyber risk underwriting with the risk appetite and firm strategy, the PRA is following this principle and ensuring that boards take responsibility for these decisions; and

- that the regulators should exercise their functions as transparently as possible. The PRA has followed this principle by issuing a consultation on these proposals for cyber risk underwriting and including background information relating to the outcome of discussions the PRA had with key industry stakeholders that formed the basis of this consultation.

1 Section 2B of FSMA.
2 Section 2C of FSMA.
3 Section 2H(1)(b) of FSMA.
4 Section 2H(1) of FSMA.
5 See sections 2H and 3B of FSMA.

Impact on mutuals

3.10 In the PRA's opinion, the impact of the proposed SS on mutuals is expected to be no different from the impact on other firms.

Equality and diversity

3.11 The PRA is also required by the Equality Act 2010[1] to have due regard to the need to eliminate discrimination and to promote equality of opportunity in carrying out its policies, services and functions. The PRA considers that these proposals have no equality and diversity implications and as such a full assessment has not been conducted.

1 Section 149.

Appendix: Draft Supervisory Statement 'Cyber insurance underwriting risk'

Contents

1	Introduction
2	'Silent' cyber risk
3	Cyber risk strategy and risk appetite
4	Cyber expertise

1 Introduction

1.1 This supervisory statement (SS) sets out the Prudential Regulation Authority's (PRA's) expectations of firms regarding cyber insurance underwriting risk. For the purposes of this SS cyber underwriting risk is defined as the set of prudential risks emanating from underwriting insurance contracts that are exposed to losses resulting from a cyber-attack.

1.2 This statement follows a thematic review conducted between October 2015 and June 2016. The key findings were published in a letter to firms on 14 November 2016.[1]

1.3 It 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').

1.4 This statement should be read in conjunction with:

- the PRA's rules in the Solvency II sector of the PRA Rulebook, in particular rule 3.1 of the Conditions Governing Business Part, and the Insurance Senior Management Functions and Technical Provisions Parts;
- the PRA's approach to insurance supervision;[2]
- the European Insurance and Occupational Pensions Authority (EIOPA) Guidelines, particularly Guidelines 3, 17, 19, 20, 46, 47, 50, 56 and 61 on Systems of Governance and Valuation of Technical Provisions;[3] and
- Articles 9, 11, 17 and 18 of the Commission Delegated Regulation[4] of Solvency II.

1.5 This statement expands on the PRA's general approach as set out in its insurance approach document. By clearly and consistently explaining its expectations of firms in relation to the particular areas addressed, the PRA seeks to advance its statutory objectives of ensuring the safety and soundness of the firms it regulates, and contributing to securing an appropriate degree of protection for policyholders.

1.6 The PRA expects firms to be able to identify, quantify and manage cyber underwriting risk. This includes the risks emanating both from affirmative cyber insurance policies (eg data breach products), 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 statement. The PRA's expectations are split into three broad areas:

- 'silent' cyber risk (Chapter 2);
- cyber risk strategy and risk appetite (Chapter 3); and
- cyber expertise (Chapter 4).

1 'Cyber underwriting risk', www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf.
2 Available at www.bankofengland.co.uk/publications/Pages/other/pra/supervisoryapproach.aspx.
3 https://eiopa.europa.eu/Publications/Guidelines/TP_Final_document_EN.pdf.
4 Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) Text with EEA relevance.

2 'Silent' cyber risk

2.1 By its nature, 'silent' cyber risk is not always identified, managed and monitored and may be a material risk for firms.

2.2 The PRA expects that all Solvency II firms robustly assess and actively manage their insurance products with specific consideration to 'silent' cyber risk exposures. Such firms are expected to introduce measures that reduce the unintended exposure to this risk with a view to aligning the residual risk with the risk appetite and strategy that has been agreed by the board. To achieve this, besides making adequate capital provisions that clearly link with this risk, as they would for any other risk type, firms could consider any of the following (the list is not exhaustive):

- adjust the premium to reflect the additional risk and offer explicit cover;
- introduce robust wording exclusions;
- attach specific limits of cover; and
- offer cyber cover at no extra premium when the board has confirmed that a particular line of business does not carry material 'silent' cyber risk and is in line with the stated risk appetite. In this case the contract may be reworded to clarify that cyber cover is offered as part of this product.

2.3 The PRA is not a pricing regulator and does not look to design products. The aim is to enhance the ability of firms to monitor, manage and mitigate 'silent' cyber risk and to increase contract certainty for policyholders as to the level and type of coverage they hold.

3 Cyber risk strategy and risk appetite

3.1 Cyber underwriting is a key area of risk and it is important that this is reflected in the firm's strategy and risk appetite statements.

3.2 The PRA expects that all Solvency II firms that underwrite affirmative cyber insurance policies and/or those that are exposed to 'silent' cyber risk will have clear strategies on the management of the associated risks, which are owned by the board. The cyber strategy should include clearly articulated risk appetite statements with both quantitative and qualitative elements, for example defining target industries to focus on, strategy for managing 'silent' cyber risk, specifying rules for line sizes, aggregate limits for geographies and industries and splits between direct and reinsurance.

3.3 The overall strategy and associated risk appetite statements should be reviewed on a regular basis. Firms are expected to produce internal management information (MI) for review and sign-off by the board. The MI should include as a minimum:

- clear articulations of the risk appetite statements and measurements against these;
- aggregate cyber underwriting exposure metrics for both affirmative and 'silent' cyber risk;
- a confirmation that current levels of premium charged or other mitigation in place (see paragraph 2.2) is sufficient to cover claims arising from these risk exposures; and
- cyber underwriting risk stress tests that explicitly consider the potential for loss aggregation (eg via the cloud or cross-product exposures) at extreme return periods (up

to 1 in 200 years) and are consistent with the general insurance stress tests carried out periodically by the PRA.

3.4 By articulating these issues boards will understand and own the overall strategy for cyber risk and the associated prudential risks.

4 Cyber expertise

4.1 Both affirmative and 'silent' cyber risk elements present significant challenges and are underpinned by technological development. Firms active in this space are faced with the necessity of investment in knowledge and expertise.

4.2 The PRA expects that all Solvency II firms that are materially exposed to these risks understand the continuously evolving cyber landscape and demonstrate a continued commitment to developing their knowledge of cyber insurance risk. This extends to both affirmative and 'silent' elements of cyber risk. The PRA expects that this knowledge and understanding should be fully aligned to the level of risk and any growth targets in this field, and should cover all three lines of defence (business, risk management, and audit).

4.3 Regardless of any external input or advice obtained in relation to such risks, responsibility and accountability for the same remains with the firm. The firm will be responsible for the appropriate management of these risks. The PRA expects the board to have oversight of the effectiveness of the firm's risk management and controls in this area.

4.4 In this way, firms will have sufficient expertise to understand the risks associated with cyber insurance underwriting.