Institute
and Faculty
of Actuaries

Cyber Insurance Underwriting Risk – CP39/16

IFoA response to Prudential Regulation Authority

10 February 2017

About the Institute and Faculty of Actuaries

The Institute and Faculty of Actuaries is the chartered professional body for actuaries in the United Kingdom. A rigorous examination system is supported by a programme of continuous professional development and a professional code of conduct supports high standards, reflecting the significant role of the Profession in society.

Actuaries' training is founded on mathematical and statistical techniques used in insurance, pension fund management and investment and then builds the management skills associated with the application of these techniques. The training includes the derivation and application of 'mortality tables' used to assess probabilities of death or survival. It also includes the financial mathematics of interest and risk associated with different investment vehicles – from simple deposits through to complex stock market derivatives.

Actuaries provide commercial, financial and prudential advice on the management of a business' assets and liabilities, especially where long term management and planning are critical to the success of any business venture. A majority of actuaries work for insurance companies or pension funds – either as their direct employees or in firms which undertake work on a consultancy basis – but they also advise individuals and offer comment on social and public interest issues. Members of the profession have a statutory role in the supervision of pension funds and life insurance companies as well as a statutory role to provide actuarial opinions for managing agents at Lloyd's.

Institute and Faculty of Actuaries

Alex Ntelekos
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

10 February 2017

Dear Alex

IFoA response to PRA Consultation: Cyber Insurance Underwriting Risk

1. The Institute and Faculty of Actuaries (IFoA) believes cyber risk is an important new area of risk. We welcome the publication of this consultation as recognition of the PRA's concern about the matter. Members of the IFoA who work in general insurance have drafted this response.

General Comments

2. The IFoA is in general agreement with the objectives set out in the draft Supervisory Statement and believes it will raise awareness of how firms should manage the underwriting of cyber risk.

3. The IFoA supports a principles based approach to regulation, rather than setting out a detailed prescriptive approach for all insurers. There would be less need for future changes if the Supervisory Statement were principles based. Such an approach would also allow the focus of regulatory supervision to be on those firms that would not meet the principles set out in the draft statement.

4. As is the case with most new risks, firms that innovate in the area of cyber risk will receive the benefit and bear the risks from that market activity. Any regulatory activity must be proportionate for those firms. Disproportionate regulation would increase the risk that market disruptors will use new technology to develop solutions in this growing area that do not provide adequate regulatory protection for policyholders.

Silent Cyber Risk

5. We agree with the view there is significant risk associated with inadequate identification, quantification and management of 'silent' cyber risk. Consequently, there is a benefit to increasing contract certainty for policyholders in respect of the level and type of coverage they hold.

6. As such, we support the PRA's efforts to establish an 'expectation' that firms should introduce measures not only to reduce unintended exposure, but also align residual risk with the agreed risk appetite and strategy.

7. We would discourage a ‘one size fits all’ approach or overly prescribed requirements relating to the implementation of such an expectation. Policyholders will benefit if firms have flexibility to demonstrate adherence to the PRA’s expectations in a proportionate manner.

8. The list of suggested risk management actions in section 2.2 is helpful. While that list represents ideal outcomes, we would suggest a more flexible approach that enables firms to demonstrate how they meet the PRA’s expectations by addressing the risks specific to each firm.

9. The PRA and the IFoA have both addressed the concerns of the soft market recently. The impact of soft market conditions could lead to resistance to changes to contract terms (e.g. premium adjustments, exclusions, coverage limits) for fear of competitive disadvantage. Such concerns may apply to cyber risk also.

Cyber Risk Strategy and Risk Appetite

10. While the IFoA agrees the principle that boards should include cyber risk exposure within strategy and risk appetite statements, we would encourage the PRA to recognise that it may be appropriate for firms to develop strategy and risk appetite in ways that do not match the list of prescribed requirements in section 3.2. Other approaches may also meet the expectations of the principles.

11. Consequently, our view of the minimum required items in section 3.3 is that the PRA is applying a prescriptive standard that is not principles based. Firms should apply proportionate approaches to providing MI to their boards. The items listed are good examples of what firms could provide, but the list should not be a prescribed requirement.

12. We also recognise that new markets will evolve as they mature. We would encourage the PRA to review the statement in line with those market changes. There would be less need for future changes if the Supervisory Statement were principles based.

Cyber Expertise

13. The IFoA agrees with the principle that alongside strategies to grow insurance portfolios exposed to cyber risk, firms should also support investment in cyber expertise across all lines of defence. Such investment will provide better understanding of:
    - risks insured;
    - developing technology; and
    - potential loss scenarios.

14. We believe this investment will occur in any case even in the absence of any perceived regulatory intervention, proportionate or disproportionate. Many firms recognise cyber risk will provide new opportunities. Evidence of this is in the significant creativity with respect to product innovation. Our view is that insurers will seek to provide market leading, or niche, products and services to better meet the needs of policyholders. This development should lead to new wordings; coverages; increased limits and expanded service offerings alongside pure risk transfer solutions. Such developments will be seen within both standalone cyber and affirmative cyber cover within traditional lines.

15. In many firms, experts from cyber security, risk analytics, consulting, and tech start-ups, assist insurers develop better cyber risk solutions. The nature of this assistance does and will take different forms.

16. Such innovation will not benefit from prescriptive regulatory requirements. Indeed, it could force potential policyholders to seek solutions from market disruptors who have less exposure to regulatory requirements, ultimately, reducing the protections available to policyholders.

17. Whether or not they seek external expertise, firms may themselves develop appropriate levels of expertise beyond the first line of defence in order to carry out the functions outlined in sections 2 and 3. However, we would support a flexible regulatory approach that focuses on firms whose strategies are to react to the market. Such strategies could generate exposures to cyber risk without having adequate expertise, internal or external, to deal with the new exposures.

Should you wish to discuss any of the points raised in further detail please contact Philip Doggart, Technical Policy Manager (Philip.doggart@actuaries.org.uk / 0131 240 1319) in the first instance.

Yours faithfully,

C. Wil

Colin Wilson
President, Institute and Faculty of Actuaries