Institute and Faculty of Actuaries, Regulatory Board

Subject	Thematic Review Programme – Cyber risk
Meeting date	19 November 2024
Previous Steer/Approval	September 2022 – approval of thematic review topic
Related horizon scan code	HS07 (AI and Data Science – new and enhanced risks)
International issues considered?	Applicable
Author	Alan Marshall, Review Actuary
Reviewer	David Gordon, Senior Review Actuary
Purpose	Approval

A: Executive summary

1. The Actuarial Monitoring Team (AMS) has completed its thematic review looking at the work of actuaries in cyber risk.

2. This paper sets out the key findings and conclusions from the review and seeks approval for publication of the report which is planned for mid-December. The Board's response to the review findings, including any possible actions, are discussed **under a separate item.**

3. **There are findings across** the following key themes:
   - Ever increasing risk
   - Managing cyber risk
   - Playing a part in the cyber insurance market
   - Supporting actuaries
   - Research and collaboration

4. **The main conclusions are:**
   - Cyber risk is a significant risk for actuaries and the IFoA to monitor and play their part in addressing for firms. This can be through risk management skills that actuaries apply, and providing expertise in the cyber insurance market. In most instances actuaries will be working alongside other cyber risk experts.
   - The current regulatory toolkit, and lifelong learning, should be kept under review with consideration of targeted options to further support and promote IFoA members in this field. Although actuarial involvement may be lower than for some other significant risks, the materiality of the risk and the opportunities for actuaries to utilise their skills in this field, suggests further development of IFoA resources may be merited.

5. The Board is asked to **APPROVE** the draft report for publication (pre-design version), included as Appendix 1.

B: Introduction and Scope

6. Cyber risk is all around us, both in a professional context, and more widely in our day-to-day lives. However, in contrast with AI, cybersecurity may be a topic where many actuaries, whilst

aware of its critical importance, are less frequently the main experts involved in identifying and managing associated risks and opportunities.

7. That does not downplay the huge significance of cyber risk, and the importance that it is managed and mitigated appropriately for the benefit of firms and their customers. The financial system, and wider society needs such as health and security, rely heavily on the ongoing robustness of information security and in turn operational resilience. This presents an opportunity for actuaries to utilise technical and domain skills to extend influence in this field of work.

8. Cyber risk is still appearing on emerging risk assessments, but it feels like we are well past the stage of considering it as emerging, and instead should be accepting it is an established and ever-present risk to manage.

9. As the thirst for data grows ever larger, so does the risk that malicious actors will attempt to seek weaknesses in the systems and protections that firms have in place.

10. Data, and its privacy, is fundamental to the financial services world, and this brings a responsibility to ensure safety on behalf of the customers who put their faith in the sector.

11. The work of actuaries in this field may include quantifying and managing risks from potential cyber events, developing and pricing cyber risk products, and identification of potential latent risk from legacy products not intended to specifically cover cyber events.

12. This review aims to understand better where and how actuaries are involved in the management of cyber risk both within their firms, and through cyber risk products which are sold to third parties.

C: Detailed Review Findings

13. These headline findings and conclusions aim to highlight the involvement of actuaries in cyber risk work.

14. **Ever increasing risk**

    Cyber risk is a growing and significant threat. The recently published 2024 CRO Forum Emerging Risks Initiative, listed cyber as High risk, and with a current time horizon for the insurance sector. Cyber risk sits alongside and often interacts with other major global risks, climate risk, geopolitical upheaval, and AI advances.

    From a regulatory perspective, both in the UK and globally there is evidence of governments and agencies developing knowledge and resources to combat this, including expectations on firms to have appropriate controls and mitigations in place.

15. **Actuaries managing cyber risk**

    There is evidence of actuarial involvement across a range of functions and domains. Participants in our review ranged from actuaries carrying out activities on behalf of firms, including consultancy work, through to Chief Actuaries, Chief Risk Officers, and CEOs, with cyber risk management very high on each of their agendas.

Actuaries will almost always be working alongside other experts, and it is important to consider that this will have an impact on the application of standards and guidance in this space.

16. **Actuaries playing their part in the cyber insurance market**
The London market, through Lloyd's, plays a huge role in the cyber risk insurance market and there continues to be opportunities for actuaries to apply their skills in this environment. More widely the potential capacity of the market exceeds current demand, and there will be ongoing opportunities for appropriately skilled actuaries to develop in this field.

17. **Supporting actuaries**
The IFoA supports its members through standards and guidance, lifelong learning, and volunteer opportunities.

The principles of the Actuaries' Code, in particular Competence and Care, and Communication, are important given the complexity of cyber risk, requiring both robust technical skills, and the ability to communicate complexity and uncertainty to a range of stakeholders. Beyond the Code, there is no further specific IFoA regulatory standards or guidance relating to cyber risk.

At present there is cyber material in parts of the underlying curriculum for actuarial students, including specific focus in the General Insurance and Enterprise Risk Management material.

Some participants in our review indicated that both standards and guidance, and education and lifelong learning, are areas where further support could be beneficial to actuaries.

18. **Research and collaboration opportunities**
Through strong working party output, and wider contributions to cyber risk material, IFoA members have already shown how they can bring value to thought leadership and research in this area. Other actuarial bodies, and wider agencies, are active in this topic and opportunities exist to collaborate in further activity to promote work on cyber risk.

D: Conclusions

19. **The main conclusions from the report are:**
    - Cyber risk is a significant risk for actuaries and the IFoA to monitor and play their part in addressing for firms. This can be through risk management skills that actuaries apply, and providing expertise in the cyber insurance market. In most instances actuaries will be working alongside other cyber risk experts.
    - The current regulatory toolkit, and lifelong learning, should be kept under review with consideration of targeted options to further support and promote IFoA members in this field. Although actuarial involvement may be lower than for some other significant risks, the materiality of the risk and the opportunities for actuaries to utilise their skills in this field, suggests further development of IFoA resources may be merited.

20. The Board is asked to approve publication of the report and provide a steer on wording of report Foreword.

E: Appendices

- **Appendix 1**, Draft full report (pre-design version)