



Thematic Review report

Actuaries managing Cyber Risk

by Alan Marshall

Contents

Foreword	3
Introduction	4
Executive summary	5
Report structure	7
Background and context	8
Involvement of actuaries	10
Wider business and regulatory environment	15
Curriculum and lifelong learning	17
Findings and conclusions	18
Appendix 1 – Scope and approach	19
Appendix 2 – References	20
Appendix 3 – Abbreviations	22

Foreword

Neil Buckley, Lay Chair of the IFoA Regulatory Board



‘ This report provides an informative overview on both the activity of actuaries in relation to this high-profile risk and the latest developments around the world.

I welcome the publication of the Actuarial Monitoring Scheme’s (AMS) latest report, Actuaries managing Cyber risk. This continues the regulatory work of the Institute and Faculty of Actuaries (IFoA) in independently reviewing areas of work in which actuaries have significant involvement and influence. I would like to thank all those IFoA members and organisations that took part.

This report provides an informative overview on both the activity of actuaries in relation to this high-profile risk, and the latest developments around the world as firms, regulators and governments work to mitigate potential harms. At our November 2024 meeting, the IFoA Regulatory Board discussed the key findings and conclusions of the report. The Regulatory Board is keen to support actuaries already in this field and to harness opportunities to enable more actuaries to utilise their skills managing this critical and evolving risk on behalf of firms and their customers.

The Board recognises that, given actuaries are usually working alongside other cyber risk experts, there is a balance to be struck with any further IFoA specific actions, especially in relation to standards and guidance. The Regulatory Board is considering to what extent the IFoA regulatory toolkit can be best used to support actuaries in different roles, and how the Board can help keep cyber risk at the front of actuarial minds. At this stage, the Board supports the development of professional skills material in this area, and encourages ongoing consideration of learning opportunities in this field for our members. We will continue to engage with IFoA members and volunteers taking an active interest in cyber risk and encourage collaboration with global actuarial associations and other agencies to help further development of expertise and knowledge.

Neil Buckley

Lay Chair of the IFoA Regulatory Board

December 2024

Introduction

Alan Marshall, Review Actuary



‘ The aim of our thematic review is to highlight examples of where actuaries are involved in working with cyber risk.

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.

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.

The aim of our thematic review is to highlight examples of where actuaries are involved in working with cyber risk, either periodically through risk management activities, or day-to-day, where actuaries may be pricing experts providing products to the market.

Thank you to everyone who has taken part and given time to our review, this has undoubtedly helped us in assessing relevant findings to support both our members and the regulatory activity of the Institute and Faculty of Actuaries (‘IFoA’). I hope the findings and conclusions are of interest to a wide audience and we look forward to ongoing discussions and debate in this exciting field.

Alan Marshall
Review Actuary

December 2024

Executive summary

These headline findings and conclusions aim to highlight the involvement of actuaries in cyber risk work, along with key areas of potential risk.

Continually evolving risk

Cyber risk is a significant and evolving threat. The recently published 2024 **CRO Forum Emerging Risks Initiative**,¹ 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 cyber risk, including expectations on firms to have appropriate controls and mitigations in place.

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 Chief Executive Officers (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. There may be differing considerations for members involved in operational risk management activity, product and pricing specialists, and those carrying out quantification work focused on aspects such as reserving and capital

Actuaries playing their part in the cyber risk 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.

Supporting actuaries

The IFoA supports its members through standards and guidance, lifelong learning, and volunteer opportunities.

The principles of the Actuaries’ Code (the 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 are 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 learning opportunities, are areas where further support could be beneficial to actuaries.



The IFoA supports its members through standards and guidance, lifelong learning, and volunteer opportunities.

1 | 2024 CRO Forum Emerging Risks Initiative

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.



Main conclusions

1. Cyber risk is a significant and evolving 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.
2. 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 less 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.



In most instances actuaries will be working alongside other cyber risk experts.

Report structure

How this report should be read

We have set out in this report the detailed results of our thematic review. The Executive Summary sets out our key findings and conclusions; a full list can be found on **page 18**.



Findings and conclusions

The main output of this review is a series of findings based on the questionnaires and case studies submitted, conversations with actuaries in this field, and analysis of other relevant sources and material.

We have also set out conclusions highlighting where actuaries, regulators and other stakeholders might consider further work to follow-up in light of one or more of the findings.

References and abbreviations

Referenced documents or webpages are shown by footnotes on the relevant page. A full list of documents is set out in **Appendix 2**. Although abbreviations are defined when they first appear in this report, a full list is set out in **Appendix 3**.



Case studies

We have highlighted several case studies in the **Involvement of Actuaries** section of this report. These are based on the submissions made by organisations and individuals to this thematic review. In some cases, we have edited or supplemented the case studies to aid clarity or to reflect comments made in follow-up discussions.

Status of report

This report has been prepared by the IFoA Review Team and is issued by the Regulatory Board of the IFoA. Its purpose is to report on findings of the thematic review on the involvement of actuaries in managing cyber risk.

This report imposes no obligation upon members over and above those embodied in the **Actuaries' Code**² (Code) or the **IFoA Standards Framework**,³ which includes compliance with the Technical Actuarial Standards (TASs) set by the Financial Reporting Council (FRC). It is intended to be helpful to the IFoA and other regulators when considering developments in regulation. It is also intended to help actuaries in their work.

This report does not constitute legal advice. While care has been taken to ensure that it is accurate, up to date and useful, the IFoA does not accept any legal liability in relation to its content.

Review of this report

An earlier draft of the report has been subject to review by an IFoA colleague with cyber risk knowledge, who did not otherwise take part in the review.

This, along with additional editorial review, is considered by the author to meet the Work Review requirements of **Actuarial Profession Standard (APS) X2**.⁴

We wish to thank the above individuals for their review comments, although the contents of this report, in particular the findings and observations within, remain the responsibility of the IFoA Review Team.

Conflicts of interest

We are not aware of any conflicts of interest arising from the contents of this report in relation to the Review Team that carried out the work or the Regulatory Board that has commissioned the review work.

Questions about this report

We welcome questions about this report which should be sent to reviews@actuaries.org.uk.

² | The Actuaries' Code is the ethical Code of Conduct that all members of the IFoA must follow

³ | Standard Setting at the IFoA (2020)

⁴ | APS X2 – review of actuarial work

Background and context



Ransomware attacks alone reaped record payouts in 2023 and are projected to cost the world more than \$40 billion in 2024. Nation-states, major corporations, critical infrastructure providers, schools, hospitals, and ordinary citizens have all fallen victim. The ubiquity of cybercrime has normalized what was once a niche threat reserved for high-value targets.

Frank Cilluffo, McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University and **Joshua Whitman**, interim deputy director of policy at the McCrary Institute.

A sobering quote. 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 continually evolving risk to manage. 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. 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.

The cyber insurance market is estimated to be around **\$14 billion in gross written premium in 2023**,⁵ with an expectation that this will almost double in the next three to four years. However, this pales into insignificance when lined up against estimated potential losses, highlighting yet another possible insurance gap.

In this context, it is almost ironic that the highest profile IT outage in 2024 was CrowdStrike, a non-malicious event arising from issues with security patches (insured losses from the CrowdStrike outage are likely to range from **\$300 million to \$1 billion**⁶). This did highlight once again the potential impact of significant IT incidents, and the wide-ranging consequences on operational resilience of firms and the day-to-day life of the general public.

The threats associated with cyber risk continue to evolve, driven by factors such as ongoing technology advances, and activity from rogue nation states or organised crime groups. The impacts on the financial services sector can include:

- Financial, operational, and reputational damage, both from loss of data and business interruption
- Asset values being impaired following cyber-attacks and then failing to recover value
- Knock-on impacts from losses incurred in other parts of society, in particular where this leads to insurance claims (both expected and unexpected)
- Developments in the regulatory space, as governments and regulators seek to ensure firms are sufficiently operationally resilient in the event of cyber events

The 2024 CRO Emerging Risks Initiative listed cyber as High risk (the highest rating for this publication), and with a 'current' time horizon for the insurance sector. The interconnectedness with other major risks is also highlighted, in this case for geopolitical risks and the continuing advance of AI. Indeed a participant in our review, with extensive cyber risk consultancy experience, highlighted that current geopolitical tensions may to some extent be occupying

5 | Munich Re 2024 Global Cyber Risk and Insurance Survey

6 | TheActuary - Broker labels CrowdStrike outage "Kitty Cat" event

bad actors, who otherwise could be focused more on the financial sector. A recent Alan Turing Institute paper, **Generative AI in Cybersecurity**,⁷ highlighted the risk that over time there could be increased cyber threats through the use of emerging AI technologies.

Further evidence of the continued high profile of cyber risk is given in **AXA's Future Risks Report**,⁸ 2024 edition. The report highlights cyber as a 'top three' risk for both industry experts and the general population, and across different geographies.

The World Economic Forum's **Global Cybersecurity Outlook**⁹ has also highlighted the risk of growing inequities between organisations resilient to such risks and those that are not. Resilience may be lower for the small and medium enterprise population as they struggle to prioritise differing pressures on their businesses. There is a challenge here for the cyber insurance market, to help ensure mitigating cover is available to a wide range of potential customers.

Cyber risk, as is the case for many significant topics, comes with a wealth of jargon. The November 2024 joint publication by the Association of British Insurers (ABI) and Lloyd's of London, **'Components of a Major Cyber Event: A (Re) Insurance Approach'**,¹⁰ contains a very helpful glossary of terms.

This report aims to provide an updated picture of the range of functions and domains where actuaries are involved with cyber risk. The report also provides an overview of the landscape for standards and regulations relevant to cyber risk around the world.



Finding 1:

Cyber risk continues to be a growing and significant threat. The recently published 2024 CRO Forum Emerging Risk Radar, listed cyber as High risk, and with a 'current' time horizon for the insurance sector.

7 | Alan Turing Institute – Generative AI in Cybersecurity

8 | AXA Future Risks Report 2024

9 | WEF Global Cybersecurity Outlook 2024

10 | ABI and Lloyd's of London – Components of a Major Cyber Event: A(Re)Insurance Approach

Involvement of actuaries

There is a variety of evidence showing involvement of actuaries in cyber risk work. This encompasses a range of domains, including examples outside traditional areas of actuarial work.

Submissions for this review

As part of this review, we asked for submissions either on behalf of organisations, or from individuals, focusing on case studies or use cases for cyber risk, and also seeking views relating to professional standards and lifelong learning. We also reached out to individuals with extensive experience in this field for discussions to help inform our review and findings.

From the review submissions, and the discussions we held, we observed a range of examples across different areas of actuarial work:

- Risk management
- Products and Pricing
- Reserving and Capital
- Scenarios and Stress testing

The most common area of work for our participants is in relation to risk management, followed by scenario and stress testing activity. From the review submissions, and the discussions we held, it is clear that cyber risk further extends across a wide range of actuarial work.

The General Insurance domain had the greatest prevalence of actuarial involvement amongst our participants. We also received input from actuaries working in Life and Pensions.

We asked participants to what extent work in cyber risk was carried out mainly by actuaries, mainly by other experts, or a mix of both. The responses were split evenly between the latter two options, which is not surprising, given cyber risk is not a core competency of actuaries. Indeed it is encouraging that actuaries are interacting with relevant experts in a complex field.

The case studies showed work across senior management, oversight, and technical work, and across a range of actuarial domains. In drawing conclusions, it is important to think about likely differences in what actuaries may be doing in relation to operational risk management activity compared to more typical actuarial work focused on products and pricing or reserving and capital.



Case Study: Actuaries building scenarios

The assessment of cyber risk as part of wider operational risk scenario analysis, carried out as part of economic capital modelling.

This should include the identification of cyber scenarios such as distributed denial-of-service (DDOS) and ransomware attacks, how the scenario may unfold (e.g. phishing leads to all computers in a particular business unit being infected) and the types of loss that might arise (e.g. cost of re-keying in data compromised by a ransomware attack; communication costs in writing out to customers who've had their data stolen; paying for credit monitoring of affected customers and possibly compensation; regulatory fines etc.). It should also consider the state of controls and any insurance cover in place, having regard to the limitations of this (e.g. cover invalidated by using unsupported software).



Case Study: Executive level responsibility for consumer data

Whilst I don't necessarily apply actuarial knowledge and techniques in the area of Cyber Security, the firm I am CEO of holds millions of individual data records for the pension arrangements we administer or provide software as a service. Therefore Cyber risk is close to the top of our risk agenda and is actively discussed at Divisional and Group Board, Executive Committee, and Risk meetings.

Case Study: Updating cyber risk loss model

We have overhauled our attritional loss model significantly. Both the frequency and severity modules were updated, as well as moving to a more technology-driven process.

The severity module involved GLM modelling, calibrating the distribution mean and variance based on historically large observed losses. I also replicated the severity model logic in Python, allowing for a more granular understanding of the model and more efficient calibration. Finally, I helped create new technographic severity modifiers, which were used to modify the mean severity losses. These were meant to correlate with a company’s ability to mitigate losses once an attack has already started.

The other part of my work in this project involved working closely with the engineering team to integrate the new severity logic. Additionally, I worked with the data science team to integrate the frequency module programmatically.

Case Study: Cyber risk consultancy work

Areas where we have assisted clients include:

1. Pricing of cyber reinsurance contract using both actuarial analysis and vendor model outputs
2. Scenario analysis to determine the limit of cyber insurance coverages for major international airlines and hotels.

Case Study: Chief Actuary oversight

I am a Member of committees that receive presentations and reports on activities performed by the company to protect against cyber risk and the strength of the company’s protection. We also consider cyber risk in our operational risk assessments and stress and scenario testing.

Case Study: Developing a cyber risk model

The empirical cyber risk model was initially developed using a percentile method (due to absence of data) and using information from an established US cyber event data journal. The details provided include cost per data breach, probability of breach in the next two years, mean time to identify and control the damage post breach and factors that influence the cost of data breach. The journal was a critical source of information as it provides a world-wide as well as individual country-wide analysis of cyber data breaches of the past. Also, it is one of the largest databases of cyber breach incidents, available as an open-source resource. It was also validated by senior members from the Risk Management domain as part of a seminar on Enterprise Risk Management conducted by Institute of Actuaries of India (IAI)

Case Study: Managing operational cyber risk

We do not write Cyber insurance. Exposure to cyber risk is primarily through operational risk, both internal and through outsourcing.

Operational cyber risk for the Group is managed by the Chief Operating Office, through specialist Cyber and Sourcing teams, who are non-actuaries. The Actuarial Function has some involvement through the quantification of Operational risks, but is not directly involved in managing cyber risks.

In discussions with participants there were further interesting points raised:

- With the financial world now increasingly reliant on digital touchpoints, either through interactions between firms, or with customers as they access their products, cyber risk is exacerbated.
- Where actuaries have previously trained and built experience around financial risks, it is important now to ensure knowledge in operational risks, and in particular those arising from the increased digitisation of the world, including cyber.
- Scenario analysis is a strength of actuaries, as one of a number of different subject matter experts who could contribute to this, particularly on loss quantification. The best technical insights are more likely to come from cyber risk and other IT experts. This has parallels with wider operational risk scenario analysis where actuaries contribute as part of a wider multidisciplinary world.
- Commercial exposure to cyber-attacks may increase significantly in the scenario that the geopolitical situation stabilises to any extent. Bad actors are likely to be currently tied up in state-sanctioned activities and their skills could be easily transferred to criminal activity. Actuaries, and other cyber experts, need to think ahead to address this potentially enhanced risk.
- There is a range of third-party 'vendor' models available to help measure cyber risk. However, there is a lack of consistency in terms of the output, and updates to models can lead to significant changes in outcomes.
- Risks to life insurers historically focussed on financial risks of providing options and guarantees to policyholders. Certain regulatory changes, coupled with firms de-risking product design, has accelerated the digitalisation of the industry through distribution, servicing, and outsourcing. This means operational risks such as cyber, systems resilience, and fraud are an increasing share of the risk environment for today's insurers.



Finding 2:

There is evidence of actuarial involvement across a range of functions and domains. Participants in our review ranged from actuaries carrying out risk management and quantification activities on behalf of firms, including consultancy work, through to Chief Actuaries, Chief Risk Officers, and Chief Executive Officers involved in oversight roles. Within this, actuaries will almost always be working alongside other cyber experts.

Standards and Guidance considerations

From an IFoA perspective, the Code must be followed by members for all actuarial work. Two of the most relevant principles of the Code worth highlighting in this context are:

- Principle 2 of the Code which states that "Members must carry out work competently and with care" and "must ensure that they have an appropriate level of relevant knowledge and skill to carry out a piece of work."
- Principle 6 of the Code states that "Members must take reasonable steps to ensure that any communication for which they are responsible or in which they have a significant involvement is accurate, not misleading, and contains an appropriate level of information."

In the UK, existing FRC technical standards also may apply to some work by actuaries in this domain, with **TAS 100**¹¹ and the accompanying **model guidance**¹² most relevant. For non-UK members, recognised standards in the relevant jurisdictions will apply, to the extent that consistency is achieved with the requirements of International Actuarial Association **ISAP 1**.¹³

We asked participants in the review their views on the current technical, professional, and ethical regulatory material in place, and how it applies to cyber risk work.

The vast majority responded that these were either 'Just right', or 'Too little' (with only one response indicating 'Too much'). The sample size is not in any way significant; however it is interesting that there was noticeable feedback that more support may be helpful in this area.

11 | FRC Technical Actuarial Standard 100: General Actuarial Standards

12 | FRC Technical Actuarial Guidance: Models

13 | IAA ISAP 1 - General Actuarial Practice

Responses and discussion points included the following:

“Cyber risk domain has progressed considerably, and the actuarial standards have just about been able to cope up with the dynamics. However, there is scope to further drill down into the subject and explore many areas to upgrade the standards in relation to cyber risk.”

“I don't believe TAS should be applied automatically to cyber risk modelling and management as more often than not, this will be assessed and managed by a multidisciplinary team involving IT and cyber experts and non-Actuarial risk managers as well as actuaries. Some aspects of TAS may be useful guidance in modelling and reporting on cyber risk, but should not be mandatory.”


“I'm simply not aware of specific standards hence assume it's light. Generally speaking it's a complex area and we could support professionals in embracing a new way of looking at fast paced risks.”

“Current standards are right for the current operating model at our firm. If actuaries take a greater role in managing cyber risk in future, then more might be required in the standards.”

In our discussions, one participant said that the Code was very important to them in their role, focused on the professional duty to protect customer data. Another participant thought that there may be differing considerations depending on the role of the actuary, and the extent to which competitiveness with other disciplines may be impacted by differences in professional regulatory burdens.

The responses show that actuaries, and their organisations, see standards and guidance as important aspects of how we support our members working in cyber risk management. It is also important to bear in mind that as indicated above, the vast majority of the time actuaries will be working alongside other experts and that this will have an impact on the application of standards and guidance in this space.

The principles of the 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 existing specific IFoA regulatory material relating to cyber risk.

 **Finding 3:**

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. At present relevant IFoA regulatory material for cyber risk is limited to the application of Code principles.

Examples of IFoA member-driven activity

There are several IFoA initiatives where our members have driven relevant activity in cyber risk:

- Working party
- Conference sessions
- Webinars
- Research papers

The Cyber Risk Investigation working party, sponsored by the Risk Management practice board, was formed in 2015 and has been an exceptionally active group since then.

The weight of material produced by the group is impressive, focused principally on the risk management aspects of cyber risk, and how to quantify the risk for a variety of uses. One particular highlight was the publication in the British Actuarial Journal of the paper, **Cyber operational risk scenarios for insurance companies**,¹⁴ which aimed to drive greater awareness of cyber as an operational risk for insurers through a proposed framework for scenario development and worked examples.

14 | British Actuarial Journal 2019 – Cyber operational risk scenarios for insurance companies, Egan R, Cartagena S, Mohamed R, et al

Further examples of output from the group, covering topics such as silent (non-affirmative) cyber and pension scheme cyber risk, can be found on the **working party page** on the IFoA website.

During 2024 both the GI Spring Conference and GIRO had sessions where challenges related to reserving for cyber risk have been explored. The abstracts for these sessions are set out below:

- Focus on the current UK cyber insurance covers and market, outlines the key challenges, and analyses reserving methodologies to address them. It discusses different risk mitigation strategies that can help minimise cyber risk exposure, which could, in turn, reduce reserve uncertainty.
- As cyber risks are an evolving territory, our session intends to cover cybercrime, cyber insurance, and reserving challenges, with a key focus on:
 - History of cyber risks and insurance over the last 20 years
 - Challenges for insurers due to the ever-evolving nature of losses and lack of historical data
 - Risk assessment and regulatory requirements
 - Modelling techniques for effective reserving, tail risk assessment including allowance for cyber catastrophes
 - Risk mitigation strategies and impact on reserving

The Annals of Actuarial Science includes the 2024 paper, **Modeling and management of cyber risk: a cross-disciplinary review**,¹⁵ which highlights the recent advancements in cyber risk prediction, modelling, management, and insurance, across different domains including actuarial science.

A further publication, co-authored by IFoA members, **Operational Resilience in the UK Financial Sector: Practical Guidance**,¹⁶ is not wholly focused on cyber risk - it does however provide significant context for this in the consideration of operational resilience. Additionally, the paper provides an excellent summary of relevant global regulation.

Global actuarial activity

In addition to the activity of IFoA members, there is also extensive work and research material originating from the global actuarial community.

In Australia, the Actuaries Institute published a green paper, **Cyber Risk and the Role of Insurance**.¹⁷ This provides excellent background information on cyber risk, and then sets out in more detail the importance of the cyber insurance market.

In North America, the paper **Quantification of Cyber Risk for Actuaries**,¹⁸ a collaboration between the Casualty Actuarial Society, the Society of Actuaries, and the Canadian Institute of Actuaries, provides a technical grounding and framework to analyse the cyber risks of an organisation.

Further technical content is provided in the European Actuarial Journal paper, **Modeling and pricing cyber risk**,¹⁹ providing a comprehensive overview of the topic.

A recent paper from the German Association of Actuaries journal, **Actuarial Insights on Cyber Risk: Challenges and Opportunities for Today's Economy**,²⁰ contains interesting insights on the challenges arising from a lack of data.

The American Academy of Actuaries has developed a **Cyber Risk toolkit**²¹ which has several modules for actuaries to explore.

In conjunction with the IFoA material highlighted above, these are excellent resources to provide actuaries with a solid grounding in cyber risk.

The extent of wider global activity in the actuarial community also highlights the opportunity for collaboration and sharing of best practice and insights.



Finding 4:

IFoA members carry out significant additional activity and research in the field of cyber risk. There are a number of examples of helpful learning material to support members seeking to develop in this topic.

15 | Annals Of Actuarial Science – Modeling and management of cyber risk: a cross-disciplinary review, He R, Jin Z, Li JS-H

16 | Operational Resilience in the UK Financial Sector: Practical Guidance Klumpes, P. J. M., Chanon, R., Habahbeh, L., & Mann, S. (2024)

17 | Actuaries Institute – Cyber Risk and the Role of Insurance

18 | CAS/SOA/CIA – Quantification of Cyber Risk for Actuaries

19 | European Actuarial Journal 2023 – Modeling and pricing cyber risk, Awiszus, K., Knispel, T., Penner, I. et al.

20 | German Association of Actuaries – Actuarial Insights on Cyber Risk

21 | American Academy of Actuaries – Cyber Risk toolkit

Wider business and regulatory environment

There are several types of agencies influencing the business and regulatory environment for cyber risk across international jurisdictions, with differing responsibilities and objectives:

- **Government sponsored agencies** which are responsible for protection and risk mitigating activities, including the promotion of best practice for business and the wider public
- **Regulators** whose main focus is implementing and monitoring compliance with regulations designed to ensure robust business practices and risk management, including operational resilience
- **Independent agencies** which focus more on research, highlighting emerging risks, and again the promotion of best practice

All of these will have relevance to the work of actuaries in cyber risk. Taken together, there exists substantial focus and resources targeted at cyber risk and security, helping to mitigate, to some extent, the material risks which are present globally, and to increase our understanding of this subject.

United Kingdom

In the United Kingdom, the **National Cyber Security Centre (NCSC)** is tasked with supporting the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. The NCSC carries out the following:

- provides practical guidance on cyber security
- responds to cyber security incidents
- uses industry and academic expertise to enhance the UK's cyber security capability
- reduces risks to the UK by securing public and private sector networks

From a financial services regulatory perspective, both the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have focused on cyber risk management, and more widely, operational resilience to mitigate and recover from cyber-attacks. The PRA has also included cyber risk in scenario and stress testing exercises for banks and insurers.

Lloyd's of London also plays a role in central oversight of cyber insurance activity, including the setting of relevant 'Realistic Disaster Scenarios' (RDS) for syndicates to apply to portfolios to test resilience under stress. The **2024 RDS**²² contains a number of cyber examples. In November 2024 Lloyd's also co-published a paper with the ABI, 'Components of a major cyber event', which sets out common elements to consider for such events, focusing on an insurance perspective.

The Pensions Regulator (TPR) has published **cyber security principles**²³ for pension schemes, and has called on pension scheme trustees to report significant cyber-related incidents to TPR on top of existing reporting requirements.

United States

The United States has major governmental agencies with a focus on cyber security, with both the **Cybersecurity and Infrastructure Security Agency (CISA)**, and the **National Institute for Science and Technology (NIST)**, having responsibilities in this space. The CISA leads the effort to understand, manage, and reduce risk to the cyber and physical infrastructure, and leads on international collaboration. NIST seeks to help organisations better understand and improve their management of cyber risk, with frameworks in place to assist with this. Additionally, the National Association of Insurance Commissioners (NAIC) supports state insurance commissioners to effectively regulate the insurance industry and protect consumers, and provides **information on the cyber insurance market**.²⁴

22 | Lloyd's 2024 Realistic Disaster Scenarios

23 | TPR - Cyber security principles for pension schemes

24 | NAIC - Report on the Cyber Insurance Market

European Union

The European Union Agency for Cybersecurity, ENISA, carries out work to drive a consistently robust level of cybersecurity activity across Europe. The 2019 **EU Cybersecurity Act**²⁵ is a key piece of legislation setting out requirements, including certification of cybersecurity products and services, strengthening the role of the ENISA, and setting cybersecurity standards and guidelines. The European financial regulator EIOPA produced a **report on cyber risks for insurers**²⁶ providing information about cyber risk for the European insurance sector, both from an operational risk management perspective and an underwriting perspective. EIOPA also liaises with other EU agencies in promoting cyber security.

Singapore

Singapore's financial regulator, the Monetary Authority of Singapore (MAS), has strategy and guidance in place covering the regulation of cyber security and technology risk management across the financial sector. This is provided through a range of **resources and initiatives** to encourage sound risk management practices and robust business continuity plans.

Internationally

Multiple agencies are active in researching and encouraging best practices when it comes to cyber risk:

- The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. Its aim is to promote effective and globally consistent supervision of the insurance industry. In 2023 the IAIS published a **global insurance market report**²⁷ which covered the cyber insurance market, the resilience of the insurance industry to cyber risk, and the wider topic of financial stability.
- The Organisation for Economic Co-operation and Development (OECD), which promotes best practice policy across a range of topics, has various Digital Security **publications and recommendations**. One of their key messages encourages *"An economic and social approach to cybersecurity is essential to reduce cyber risk, maintain trust and increase the resilience of our economies"*.

- As highlighted earlier in this report, the World Economic Forum (WEF) 2024 publication, Global Cybersecurity Outlook 2024, highlights the risk of cyber inequity between organisations that are cyber resilient and those that are not. The issue of cyber skills talent shortage is also emphasised.



Finding 5:

Both in the UK and globally governments and agencies have developed knowledge and resources to combat cyber risks, and continue to make enhancements as the threat increases. There are also increasing expectations on firms to have appropriate controls and mitigations in place.



Finding 6:

Combining the IFoA, wider global actuarial community, and extensive resources available through other international agencies, there exists a wealth of information to inform actuaries on cyber risk and security.

25 | European Union Cybersecurity Act

26 | EIOPA – Cyber Risk for insurers: challenges and opportunities

27 | IAIS – GIMAR Special topic edition: Cyber

Curriculum and lifelong learning

In recent years the IFoA has developed the assessment curriculum and encouraged lifelong learning resources to cover developments in cyber risk.

In recent years the IFoA has developed the assessment curriculum and encouraged lifelong learning resources to cover developments in cyber risk. The IFoA continually reviews the curriculum and supporting resources, to ensure they remain relevant and provide our qualifying actuaries with a solid grounding in key risks and topics.

At present the assessment curriculum covers cyber risk at a high-level across the Specialist Principles and Specialist Advanced subjects, with some additional focus in General Insurance and Enterprise Risk Management. For the latter additional cyber risk case study material has been introduced for actuaries participating in the Chartered Enterprise Risk Actuary (CERA) seminar.

Earlier in the report we highlighted the significant lifelong learning material that is available, either through the IFoA, or from wider sources. This provides a wide range of learning opportunities for actuaries, from a relatively high-level introduction to more detailed material on some of the specialised aspects of cyber risk.

Participants in the review indicated that this is an area where further development would benefit members seeking to apply skills in cyber risk. There were suggestions to extend the material that the IFoA provides, and for consideration of curating relevant material for ease of access. One response suggested that where more specialised knowledge is required, alternative providers of learning material for cyber risk and cybersecurity may be an option.





Finding 7:

At present there is some cyber risk material in parts of the underlying curriculum for actuarial students, including some additional focus in the General Insurance and Enterprise Risk Management material. Participants in our review indicated that education and lifelong learning is an area where further support could be beneficial to actuaries.

Findings and conclusions

A full list of our findings and conclusions is given in the table below. These are set out in the order they appear in this report.

 Findings:	
1	Cyber risk continues to be a growing and significant threat. The recently published 2024 CRO Forum Emerging Risk Radar, listed cyber as High risk, and with a 'current' time horizon for the insurance sector.
2	There is evidence of actuarial involvement across a range of functions and domains. Participants in our review ranged from actuaries carrying out risk management and quantification activities on behalf of firms, including consultancy work, through to Chief Actuaries, Chief Risk Officers, and Chief Executive Officers involved in oversight role. Within this, actuaries will almost always be working alongside other cyber experts.
3	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. At present relevant IFoA regulatory material for cyber risk is limited to the application of Code principles.
4	IFoA members carry out significant additional activity and research in the field of cyber risk. There are a number of examples of helpful learning material to support members seeking to develop in this topic.
5	Both in the UK and globally governments and agencies have developed knowledge and resources to combat cyber risks, and continue to make enhancements as the threat increases. There are also increasing expectations on firms to have appropriate controls and mitigations in place.
6	Combining the IFoA, wider global actuarial community, and extensive resources available through other international agencies, there exists a wealth of information to inform actuaries on cyber risk and security.
7	At present there is some cyber risk material in parts of the underlying curriculum for actuarial students, including some additional focus in the General Insurance and Enterprise Risk Management material. Participants in our review indicated that education and lifelong learning is an area where further support could be beneficial to actuaries.

 Conclusions:	
1	Cyber risk is a significant and evolving 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.
2	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 less 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.

Appendix 1: Scope and approach

This Thematic Review was announced in December 2022 as:



Cyber Risk

Cyber risk is now an established risk being managed by firms employing actuaries.

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.

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.

Review activity commenced in April 2024, and completed in November 2024.

The IFoA website provides more information on **the work of the AMS Team**.

Review methodology

The review was carried out in a number of ways:

- Collecting information from organisations and individuals through a review questionnaire
- Asking for examples of material produced by actuaries
- Researching the business and regulatory environment
- A high-level review of the current actuarial education and lifelong learning material relevant to cyber risk management
- Follow-up interviews with actuaries at participating organisations to understand the context of the questionnaire responses and any work examples received
- Further interviews with individuals knowledgeable in this field.

Submissions and participation

We received 11 submissions to our review and carried out a number of supporting interviews. Thank you to all participants for their invaluable input, and particular thanks to Vivesh Gosrani for his time and expertise.

Appendix 2: References

No.	Title	Author
1	Emerging Risks Initiative 2024	CRO Forum
2	The Actuaries' Code	IFoA
3	Standard Setting at the IFoA (2020)	IFoA
4	APS X2 – review of actuarial work	IFoA
5	2024 Global Cyber Risk and Insurance Survey	Munich Re
6	Broker labels CrowdStrike outage “Kitty Cat” event	TheActuary
7	Generative AI in Cybersecurity	The Alan Turing Institute
8	Future Risks Report 2024	AXA
9	Global Cybersecurity Outlook 2024	WEF
10	Components of a Major Cyber Event: A(Re)Insurance Approach	ABI and Lloyd's of London
11	Technical Actuarial Standard 100: General Actuarial Standards	FRC
12	Technical Actuarial Guidance: Models	FRC
13	ISAP 1 - General Actuarial Practice	IAA
14	Cyber operational risk scenarios for insurance companies	British Actuarial Journal 2019, Egan R, Cartagena S, Mohamed R, et al
15	Modeling and management of cyber risk: a cross-disciplinary review	Annals of Actuarial Science, He R, Jin Z, Li JS-H
16	Operational Resilience in the UK Financial Sector: Practical Guidance	Klumpes, P. J. M., Chanon, R., Hababbeh, L., & Mann, S. (2024)
17	Cyber Risk and the Role of Insurance	Actuaries Institute
18	Quantification of Cyber Risk for Actuaries	CAS/SOA/CIA

No.	Title	Author
19	Modeling and pricing cyber risk	European Actuarial Journal 2023, Awiszus, K., Knispel, T., Penner, I. et al
20	Actuarial Insights on Cyber Risk	German Association of Actuaries
21	Cyber Risk toolkit	American Academy of Actuaries
22	2024 Realistic Disaster Scenarios	Lloyd's of London
23	Cyber security principles for pension schemes	TPR
24	Report on the Cyber Insurance Market	NAIC
25	Cybersecurity Act	EU
26	Cyber Risk for insurers: challenges and opportunities	EIOPA
27	GIMAR Special topic edition: Cyber	IAIS

Appendix 3: Abbreviations

Abbreviation	Full term
AAE	Actuarial Association of Europe
ABI	Association of British Insurers
AI	Artificial Intelligence
APS	Actuarial Profession Standard
CRO	Chief Risk Officer
CEO	Chief Executive Officer
DDOS	Distributed denial-of-service
FCA	Financial Conduct Authority
FRC	Financial Reporting Council
GI	General Insurance
GLM	Generalised Linear Model
IAA	International Actuarial Association
IAIS	International Association of Insurance Supervisors
IFoA	Institute and Faculty of Actuaries
ISAP	International Standard of Actuarial Practice
IT	Information Technology
MAS	Monetary Authority of Singapore
NAIC	National Association of Insurance Commissioners
NCSC	National Cyber Security Centre

Abbreviation	Full term
OECD	Organisation for Economic Co-operation and Development
PRA	Prudential Regulatory Authority
TAS	Technical Actuarial Standard
WEF	World Economic Forum



Beijing

Room 512 · 5/F Block A · Landgentbldg Center · No. 20 East Middle 3rd Ring Road
Chaoyang District · Beijing · 100022 · People's Republic of China

Tel: +86 (10) 6611 6828

Edinburgh

Spaces · One Lochrin Square · 92 Fountainbridge · Edinburgh · EH3 9QA

Tel: +44 (0) 207 632 2100

London (registered office)

1-3 Staple Inn Hall · High Holborn · London · WC1V 7QJ

Tel: +44 (0) 207 632 2100

Malaysia

Arcc Spaces · Level 30 · Frankfurt Room · The Gardens North Tower
Lingkaran Syed Putra · 59200 Kuala Lumpur

Tel: +60 12 591 3032

Oxford

Belsyre Court · 1st Floor · 57 Woodstock Road · Oxford · OX2 6HJ

Tel: +44 (0) 207 632 2100

Singapore

Pacific Tech Centre · 1 Jln Kilang Timor · #06-01 · Singapore · 159303

Tel: +65 8778 1784