European Insurance and Occupational Pensions Authority

EIOPA Workshop on Cyber Insurance

Opening Speech by Gabriel Bernardino, Chairman of the European Insurance and Occupational Pensions Authority (EIOPA)

Frankfurt am Main, 1 April 2019

It is a great pleasure to welcome all of you this afternoon to the first EIOPA Workshop on Cyber Insurance.

Great to see that we have full house and many of you followed our invitation or wanted to attend!

I learnt we have in addition around 30 participants following the discussions remotely via WebEx. Hallo also to them, I understand you can see all of us!

The significance of the European cyber insurance industry is growing.

New regulations, as well as new technological developments and further materialisation of incidents are expected to raise awareness and foster demand for cyber insurance in the coming years.

The idea of this workshop was originated based on the main conclusion of EIOPA's Report on "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies". One of the conclusions was that there is a clear need for a deeper understanding of cyber risk.

Therefore, I welcome all of you, all crucial players in this segment, to a dialogue aiming at addressing the key challenges regarding cyber insurance underwriting identified in the EIOPA report.

For this purpose, the workshop is organized in two parts:

- The first part will consist of two presentations on relevant challenges followed by a discussion with the audience. They cover the “Broadness of coverage, terms and conditions and non-affirmative risks” and “How to improve understanding of cyber risks and align with clients’ needs”.
- The second part will consist of two parallel breakout sections, in which the audience will be divided into two groups and invited to discuss topics in a more focused way, more precisely accumulation risk and difficulties in properly quantifying risks and risk of mispricing.

I would like to take this opportunity to express my sincere thanks to the colleagues taking care of the organisation and in particular to our honourable speakers and moderators.

In my opening remarks, I want to touch upon **cyber insurance as an enabler of the digital economy.**

The digital transformation of how we work, live and do business has created huge opportunities for innovation and efficiency. However, our increased dependency on digital technologies also carries information security and privacy risks. Cyber security and cyber risk are at the forefront of the concerns of economic operators and public authorities. And, cyber risk is quickly becoming part of the digital economy environment.

The innovation and efficiency brought with the use of new technologies and high volumes of information will only become a reality if we find collective solutions to deal appropriately with cyber risk. That calls for an appropriate **framework for cyber risk assessment, resilience and coverage**.

The insurance sector has an important role to play in establishing good risk management practices and the associated coverage. Insurance can make a valuable contribution to managing cyber risk faced by businesses, organisations and individuals. A well-developed cyber insurance market can help:

- To raise awareness of businesses to the risks and losses that can result from cyber-attacks
- To share knowledge of good cyber risk management practices
- To encourage risk reduction investment - by establishing risk-based premiums
- To facilitate responses to and recovery from cyber-attacks

In this context, EIOPA is interested in maintaining a close dialogue with market participants and other stakeholders on the main challenges for building up **the insurance industry's role in cyber risk assessment, resilience and coverage**.

Overall, we identify two main challenges: Quantifying cyber risks and Covering cyber risks.

1. Quantifying cyber risks

A number of factors hinder the development of sound actuarial risk and cost assessment techniques, and consequently have a negative impact on the supply of insurance coverage for cyber risk:

- The limited availability of data on past cyber incidents
- The rapid pace of change in the nature of cyber risk
- The uncertainty about the effectiveness of different security technologies in terms of risk reduction
- The potential for accumulated losses

Efforts need to be made to ensure a path from the current scenario-based modelling of cyber risk to the development of robust probabilistic models.

We would like to discuss with the different stakeholders what could be done to improve the insurance industry's capacity to quantify properly cyber risks.

In this context, a number of questions deserve appropriate reflection and an adequate response:

- Is it possible and desirable to harmonise claims and incident data?
- Should a specific categorisation of cyber incidents be part of that harmonisation?
- How to overcome the concerns related to the sharing of incident data within the insurance industry and between the public and private sectors?
- How can an EU data repository be build up?
- How to ensure that an eventual data repository protects anonymization and is managed under strong security controls?
- How can the industry develop best practices on the assessment of the potential for accumulation risk?

2. Covering cyber risks

The coverage of cyber risks by the insurance industry is developing at a fast pace. Nevertheless, more work needs to be done in terms of products, services and risk transfer mechanisms. In the coming months, we would like to discuss questions like:

- Is there an advantage in the development of market and/or regulatory initiatives aimed at ensuring standardisation of coverage terms and conditions?
- Will standardization of coverage help to develop appropriate mechanisms to transfer cyber risks to the reinsurance market and capital markets?
- Should pooling mechanisms be established to cover peak risks?
- Is there a role for a public backstop to cover the extreme events and deal with cyber terrorism and cyber warfare?
- As the cyber insurance markets mature, should cyber insurance become mandatory?

Conclusion

The EU strategy for the digital single market notes that making the EU's single market fit for the digital age requires tearing down unnecessary regulatory barriers and moving from individual national markets to one single EU-wide rulebook. This challenge is also present in the cyber insurance area.

We should work together to establish an EU framework for the **insurance industry's role in cyber risk assessment, resilience and coverage.** This would provide a further level of security for companies and consumers in the digital economy.

I wish you all an interesting afternoon with vivid and controversial discussions.

Thank you.