European Insurance and Occupational Pensions Authority

Workshop on Cyber Insurance

Summary of the workshop on cyber insurance organised by the European Insurance and Occupational Pensions Authority (EIOPA) on 1 April 2019 at EIOPA's premises in Frankfurt am Main

On 1 April 2019, the European Insurance and Occupational Pensions Authority (EIOPA) hosted a Workshop on Cyber Insurance. More than 100 representatives from the insurance industry, brokers, consumers, regulators, think tanks and other stakeholders participated. The workshop continued the structured dialogue with the insurance industry on cyber insurance, which resulted in a first EIOPA report published in 2018. One of the key conclusions of this report was the clear need for a deeper understanding of cyber risk. The goal of the workshop was to discuss and identify possible solutions to address the challenges the European cyber insurance market is facing. Specifically, the workshop focused on two main challenges: cyber risks coverage and quantification of cyber risks.

In his opening remarks, EIOPA's Chairman Gabriel Bernardino stressed the importance of cyber insurance as an enabler of the digital economy. The increased dependency on digital technologies carries significant information security and privacy risks. Consequently, cyber risk is quickly becoming an integral part of the digital economy environment. Finding collective solutions to deal appropriately with cyber risk calls for an equally appropriate framework for cyber risk assessment, resilience and coverage. A well-developed cyber insurance market can play a key role in this, for instance:

- 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

Furthermore, he stressed that, as also noted in the European Union strategy for the digital single market, making the single market fit for the digital age requires tearing down unnecessary regulatory barriers and moving from individual national markets to one single European Union-wide rulebook. This challenge is also present in the cyber insurance area. All parties should work together to establish such a European Union framework addressing 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.

Plenary sessions on "Covering cyber risks: broadness of coverage and aligning with clients' needs"

Representatives from the insurance industry and corporate policyholders gave a short introductory presentation setting the scene, describing recent trends and providing different perspectives. The session started with an overview of the different type of cyber insurance coverages observed in the market, highlighting that the broadness of coverage of cyber risks has gradually evolved over time and increasingly includes more preventive and advisory services. Participants shared the view that the broadening of cyber coverage and removal of standard cyber exclusions could become a growing concern for the industry and could lead to more accumulation risk in the future.

Another key issue discussed was the treatment of 'silent' cyber risk: cyber risks that are either not explicitly included or excluded in policies. Silent cyber risk exposure is one particular channel trough which cyber could become a peril for the industry. At the same time, it is also an area, which requires a clear management of policyholder expectations to provide clarity what is covered in traditional policies and to avoid legal uncertainty. Participants recognized that a clear consumer perspective is needed to better align with the needs of Small and Medium-Sized Entities (SMEs) and individuals in particular.

The key take-aways from the discussions going forward are:

- It is important to enhance transparency and standardisation of cyber coverage to improve comparability of cyber insurance, in particular for SMEs
- There is a clear need to address silent cyber risk in traditional policies and remove contractual uncertainty
- Insurers could play a role in improving cyber resilience of companies
- Regulators could act as enablers by setting clear standards on cyber security and cyber risk and help raise awareness
- The role of a government back-stop for systemic cyber events and cyber warfare should be considered

Break-out sessions on Quantifying cyber risk and accumulation risk

Participants discussed the challenges insurers are facing in properly quantifying cyber risk and accumulation risk in two break-out sessions. Obstacles relate not only to the limited historical

data and limited data sharing on cyber incidents for affirmative cyber risk, but also to the difficulties in assessing accumulation risks for silent cyber exposures. Participants acknowledged that a lack of resources and expertise pose further challenges to quantifying cyber risks, especially in light of the dynamic and quickly evolving nature of cyber risk. While they saw a role for regulators and supervisors to foster data collection and sharing, it was stressed that this should not hamper the development of market-based solutions.

The key take-aways from the discussions going forward are:

- Collaboration among stakeholders and data-sharing are key
- Extending notification requirements to other types of cyber incidents to foster data collection should be considered
- A 'Cyber' database with anonymized data on cyber incidents, based on common definitions to facilitate data collection and data sharing, should be considered. This database can be based on a European initiative ahead of any international developments.
- It is important to enhance the use of scenario analysis to assess accumulation risk for insurers
- Common standards and a taxonomy for both cyber risk measurement and reporting purposes could be developed. Again, this can be based on a European initiative.

The agenda of the Workshop and presentations can be obtained here.

EIOPA will incorporate the outcome of the workshop in its ongoing work on cyber insurance . EIOPA is committed to continuing the dialogue with stakeholders to address the challenges and opportunities for the European Cyber Insurance market.