EIOPA calls for a sound cyber resilience framework

The European Insurance and Occupational Pensions Authority (EIOPA) published today the report on "Cyber Risk for Insurers – Challenges and Opportunities".

The increasing frequency and sophistication of cyber attacks, the fast digital transformation and the increased use of big data and cloud computing make insurers increasingly susceptible to cyber threats, in particular considering the amount of confidential policyholder information insurers are possessing. This calls for a sound cyber resilience framework for insurers.

On the other hand, the digital economy and the advance of technology offer opportunities to cyber underwriters. Appropriate cyber insurance coverages can make a valuable contribution to manage cyber risk faced by businesses and organisations. A well-developed cyber insurance market can play a key role in enabling the transformation to the digital economy.

Insurers play a key role in this transformation: not only are insurers susceptible to cyber threats directly themselves, but they also offer coverage for cyber risk through their underwriting activities. This report analysed cyber risk from both angles based on responses from 41 large (re)insurance groups across 12 European countries with the aim to further enhance the level of understanding of cyber risk for the European insurance sector.

The findings confirm the need for a sound cyber resilience framework for insurers and identified the key challenges faced by the cyber underwriters. In particular, clear, comprehensive and common requirements on the governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services. This would include a consistent set of definitions and terminology on cyber risks to enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could further enhance the cyber resilience of the insurance sector. Ultimately, further actions to strengthen the resilience of the insurance sector against cyber vulnerabilities are essential, in particular considering the dynamic nature of cyber threats.

Regarding the cyber insurance market, the report finds that, although still small in size, the European cyber insurance industry is growing rapidly, with an increase of 72% in 2018 in terms of gross written premium for the insurers surveyed in the report, amounting to EUR 295 million in 2018 compared to EUR 172 million in 2017. However, non-affirmative cyber exposures (where cyber risk is neither explicitly included nor excluded within an insurance policy) remain a source of concern. While common efforts to assess and address non-affirmative cyber risks are under way, some insurers have adopted a 'wait-

and-see’ approach to address non-affirmative cyber risk, where the implementation of actions plans to address non-affirmative exposure depends on the materialization of future events. Therefore, further effort is needed to tackle properly non-affirmative cyber exposures to address the issue of potential accumulation risk and provide clarity to policyholders.

Finally, enhanced data collection on cyber incidents and losses should allow insurers to manage and price their affirmative cyber risk exposures more effectively. Having common and harmonized standards for both cyber risk measurement and cyber incident reporting purposes could greatly facilitate this. To this end, creating a European-wide cyber incident-reporting database, based on a common taxonomy, could be considered.

Background

This report is based on the responses of 41 large (re)insurance groups across 12 European countries: Austria, Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Spain, Sweden and United Kingdom.

The sample under consideration is very similar to the one of the EIOPA 2018 Insurance Stress Test, representing a market coverage of around 75% of total consolidated assets.

The only difference is the non-participation of one group included in the sample for the Stress Test 2018 exercise.