June 2020

Key messages on EIOPA's cyber underwriting strategy

- Insurance Europe welcomes EIOPA's Strategy on Cyber Underwriting and its recognition of **the role that the cyber insurance market has to play as a crucial enabler of the digital economy**. Moreover, we welcome the constructive dialogue between EIOPA and the industry, ongoing since 2018, and aimed at better understanding cyber insurance. The (re)insurance industry remains open to further collaboration on this important topic and agrees with EIOPA that the **exchange of good practices** is paramount to developing a sound EU cyber insurance market. National insurance associations have already launched various initiatives to boost cyber resilience, however further collaboration in this area can also help to **raise awareness of cyber risks** and how to handle these among companies of all sizes.

- Insurance Europe is pleased that EIOPA's strategy recognises that **the lack of quality data on cyber incidents available at European level is one of the key impediments to the continued growth of Europe's cyber insurance market.** Given the cross-border nature of cyber incidents, the availability of data at a European level is essential. However, in pursuit of EIOPA's strategic objective to promote the development of a centralised, anonymised database on cyber incidents, the following comments must be considered:

    - As a first step in increasing the volume of data available for cyber underwriting, Insurance Europe would welcome EIOPA's support in **leveraging on existing data on cyber incidents**, such as incident data gathered under the GDPR and the NIS Directive. To this end, in 2018, Insurance Europe developed a template for breach notifications under the GDPR. Data gathered in this format would be anonymised but sufficiently granular to be of use to the industry.
    - However, it must be noted that information collected under these frameworks covers only certain aspects of cyber risks. For instance, the NIS Directive requires reporting of data, but this reporting only provides a partial picture of the losses incurred. Beyond data gathered under GDPR or NIS Directive, in order to fully facilitate the development of the EU cyber insurance market, access to a greater-detailed level of data is needed. In this regard, **Insurance Europe generally supports EIOPA's ambition to act as a facilitator and welcomes active engagement with ENISA on the subject of data-sharing**. However, due consideration should be given to the practical aspects of such an initiative:
        - Importantly, it has to be kept in mind that contributing to such a centralised database will likely bring additional reporting requirements for companies, i.e. on top of the existing reporting requirements in GDPR, NIS Directive, where relevant, and at national level. Such **additional reporting requirements would be burdensome**, and it is therefore key to properly identify which data would specifically contribute to enhancing Europe's cyber resilience and should therefore be subject to a reporting requirement.
        - A centralised database of interoperable data would require standardised incident reporting. Many IT systems might be incompatible with a new reporting process, which would call for an overhaul/adaption of IT systems, something which would be financially burdensome. Furthermore, complexities may arise should IT

Insurance Europe aisbl • rue Montoyer 51, B-1000 Brussels
Transparency Register ID no.: 33213703459-54
Tel: +32 2 894 30 00
E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

systems be amended in order to comply with reporting requirements in the EU, but not in other jurisdictions (e.g. the US), as this would create inconsistencies in terms of a company's cyber incident data.
    - Any initiative should not distort competition in the market, i.e. if an insurer shares data it must gain access to an equal quantity and quality of data in return. Therefore, such a database must benefit all participants proportionately, to ensure a level playing field.
    - Once all the above conditions were met, the data shared would need to be of use to cyber insurers and could include estimated anonymised claims payment data and data on frequency and severity of incidents.
- Some Member states have developed initiatives, notably in France, where a national observatory of cyber risks was set up in order to meet the demand of national authorities, insurers and cybersecurity professionals. Such an observatory should provide visibility on past incidents and reactivity regarding future threats.

- **Insurance Europe agrees with EIOPA that it is worth exploring to what extent a common taxonomy on cyber risks could facilitate the cross-border sharing of information on cyber threats and incidents.**
    - However, there is evidence from previous engagement with cyber taxonomies that the terms rapidly become out of date and evolve to include a much wider scope and definition. A fixed taxonomy for reporting might therefore become quickly outdated. As such, the success of any EIOPA initiative depends on its level of granularity. Previous examples include cyber lexicon projects undertaken by the International Association of Insurance Supervisors (IAIS) and the Financial Stability Board (FSB) which, by the time they were finalised, were already considered to be out of date.

- Regarding EIOPA's strategic objective of "investigating cyber underwriting as a separate line of business", Insurance Europe believes that **insurers should be allowed to maintain their ability to develop a wide range of innovative cyber products**, which can vary from standalone products to aspects of a broader insurance policy. It is important to emphasise that:
    - Not all cyber coverage is sold as a stand-alone product. Cover varies greatly depending on the needs of the buyers, the type of cyber risks they are exposed to, their size, business model, and level of digitalisation.
    - Some elements of cyber risk are covered under other insurance products, such as property, director's and officer's liability Insurance (D&O) or general liability policies.
    - Undertakings should be given the freedom to manage their own accumulation of non-affirmative risk.

- Furthermore, the European (re)insurance industry is opposed to the introduction of "minimum coverage requirements per type of coverage". **The cyber insurance market is continually evolving to meet the changing landscape of risks and consumer demands**. Any standardisation of minimum requirements would, therefore, inevitably become quickly outdated and would not provide adequate guidance for businesses. As with the premature introduction of mandatory insurance, standardisation at this stage would negatively impact policyholders and insurers.
    - Policyholders forced to buy standardised products are more likely to purchase cover that is not tailored to their needs and/or to buy either more or less coverage than they actually need.
    - Insurers need the flexibility to tailor the policies to their clients' risks, and policy language is still evolving to reflect changing threats.