EIOPA STRATEGY ON CYBER UNDERWRITING

This note outlines EIOPA's strategic priorities regarding the European cyber insurance market, as part of EIOPA's broader mission to promote sound technological progress for the benefit of the European Union economy and its citizens, while safeguarding financial stability, market integrity and investors' protection. The note puts EIOPA's cyber underwriting strategy into context, discusses the work undertaken so far by EIOPA and outlines the proposed way forward.

https://www.eiopa.europa.eu/

European Insurance and
Occupational Pensions Authority

1. INTRODUCTION

EIOPA's strategic priorities take into account the European Commission's Digital Strategy, Cybersecurity Strategy[1] and FinTech Action Plan and support its ambition for a Digital Single Market[2] . The Digital Single Market is built on 3 pillars:

1. Better access for consumers and businesses to digital goods and services across Europe;
2. Creating the right conditions and a level playing field for digital networks and innovative services to flourish;
3. Maximising the growth potential of the digital economy.

A sound cyber insurance market can be a crucial enabler of the digital economy. In particular, a well-developed cyber insurance market can help:

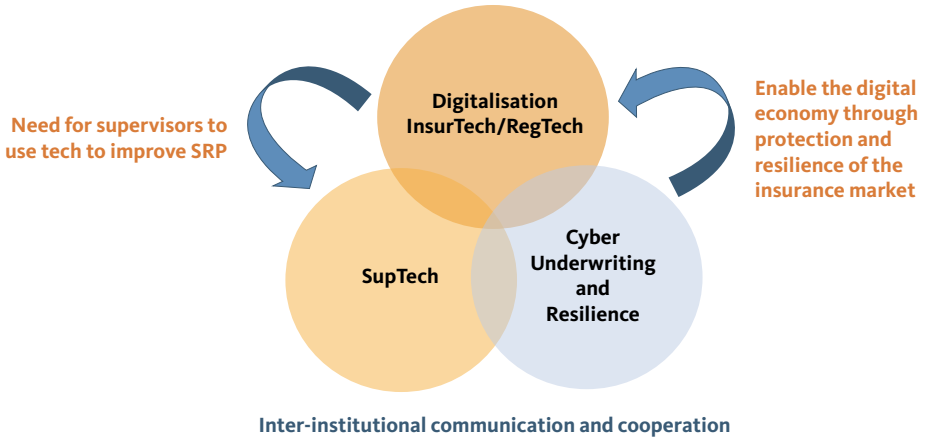
- To raise awareness of businesses to the risks and losses that can result from cyber-attacks;
- To share knowledge of good cyber security and risk management practices;
- To encourage investment in risk reduction and the use of risk-based premiums;
- To facilitate responses to and recovery from cyber-attacks.

Appropriate cyber insurance coverages, underwriting practices and sound supervision can make a valuable contribution to managing cyber risk faced by individuals, businesses and organisations and to enhance cyber resilience, ultimately enabling the digital economy. In this context, EIOPA has been developing a number of initiatives and highlighting supervisory concerns, specifically in the area of silent/non-affirmative risks as well as of accumulation of risk. It is now time to further close knowledge and data gaps regarding cyber risks and cyber underwriting in particular.

2. BACKGROUND

In the context of cyber risk many different areas are correlated and interdependent. Figure 1 provides a schematic overview of how Digitalisation in Insurance (InsurTech), SupTech and Cyber Underwriting and Resilience are related, all of which are relevant for EIOPA.

As a consequence of the digitalisation of the economy, cyber risk has been gaining increasing relevance as one of the main sources of operational risk faced by organisations, being considered the top risk in many countries. The increasing frequency and sophistication of cyber-attacks and the continued digital transformation also make insurers increasingly susceptible to cyber threats, as more and more insurance undertakings are embracing new technologies and making use of big data.



1 https://ec.europa.eu/digital-single-market/en/cyber-security

2 https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

In order to enhance the cyber security and resilience of insurance undertakings, EIOPA has, together with other ESAs, published the 'Joint Advice on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector' and the 'Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector'.

The last piece of the puzzle for EIOPA's digital and cyber strategy is cyber underwriting, i.e. the acceptance of cyber risks by insurance undertakings from its policyholders. EIOPA has been working in this area through different actions such as the reports published and workshops organised on cyber underwriting and by proposing a template to start collecting information on cyber underwriting as part of the Solvency II Reporting Review. Building on this work, this note defines an integrated strategy towards cyber underwriting and should guide EIOPA's actions on this area in the next years.

3. WORK DONE SO FAR ON CYBER UNDERWRITING

In line with EIOPA's mandate to safeguard financial stability, EIOPA has been taking several initiatives to monitor risks and identify opportunities in the context of the cyber underwriting:

- Since June 2016, analyses and assessments on cyber developments and risks are included in ***EIOPA's Financial Stability Report***.[3]
- EIOPA has initiated a dialogue with the industry to enhance the understanding of cyber risks and shed light on developments within the European cyber insurance market. This work has resulted in the **publication of the report *Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies*** [4] in August 2018.
- One of the key findings of the report confirms the fact that there is a need for a deeper understanding of cyber risk, which is a core challenge for the European insurance industry. This challenge generates or fosters other challenges, such as improper treatment of non-affirmative risks and difficulties to quantify and assess risks, among others.
- As a continuation of this structured dialogue, on 1 April 2019, EIOPA hosted a **Workshop on Cyber Insurance** to discuss and identify possible solutions to address the challenges facing the European cyber insurance market, in particular regarding covering and quantifying cyber risks, which highlighted among others the need for access to common and harmonised cyber incident reporting and development of methodologies for cyber risk measurement.[5]
- In September 2019, EIOPA published a second **report *Cyber Risks for Insurers – Challenges and Opportunities***, based on the responses from the participants in the EIOPA Insurance Stress Test Exercise 2018 to a quantitative and qualitative questionnaire on cyber risk.[6] The findings reflect that, although still small in size, the European cyber insurance industry is growing rapidly. At the same time, non-affirmative cyber exposures remain a source of concern. While common efforts to assess and address non-affirmative cyber risks are under way, the lack of quantitative approaches, explicit cyber exclusions and action plans to address non-affirmative cyber exposures suggest insurers are currently not fully aware of the potential exposures to cyber risk.

4. OBJECTIVES

To build a strong, reliable cyber insurance market requires a number of conditions, in particular:

- **Appropriate cyber underwriting and risk management practices and how its supervision needs to be in place to promote such good practices.** Regulators and supervisors should ensure that insurers apply sound underwriting and risk management tools in the area of cyber underwriting. This

3 See the reports available at: https://www.eiopa.europa.eu/content/eiopa-financial-stability-report-december-2019

4 The report is based on a survey with responses to a set of 14 qualitative questions answered by 13 (re)insurance groups located in Switzerland, France, Italy, Germany and the United Kingdom. The sample of eight insurers and five reinsurers was selected according to the expertise and current exposures in cyber insurance. The report is available at https://www.eiopa.europa.eu/content/understanding-cyber-insurance-structured-dialogue-insurance-companies

5 https://www.eiopa.europa.eu/content/eiopa-cyber-insurance-workshop

6 The report "Cyber Risks for Insurers – Challenges and Opportunities" was based on the responses of 41 large (re)insurance groups across 11 European countries representing a market coverage of around 75% of total consolidated assets. https://www.eiopa.europa.eu/content/cyber-risk-insurers-challenges-and-opportunities

would include properly managing both affirmative and non-affirmative cyber risk exposures and having adequate tools to assess and mitigate potential accumulation risk. At the same time, promoting market best practices regarding cyber risk assessments and coverage conditions can help to mitigate the moral hazard problem in order to give the policyholders the right incentives to limit the occurrence of the insured risks (e.g. pre-screening to discriminate the premium and risk-adjusted premiums).

- **Adequate assessment and mitigation tools to address potential systemic cyber and extreme risks.** Cyber risk is increasingly seen as a potentially systemic risk for the financial system and the real economy.[7] The threat of systemic risk events coming from cyber incidents might require responses from both the government and the industry to provide adequate insurance capacity in support of the real economy.[8] It is therefore important to continue to assess and monitor the extent of potential systemic cyber events and whether some risks could become uninsurable in the future, which may hamper the real economy.
- **A mutual understanding of contractual definitions, conditions and terms, for both, policyholders and insurance undertakings.** Clear and transparent cyber coverages are crucial from a consumer protection perspective. It is the role of industry and consumers associations to provide this clarity and align expectations on cyber insurance coverages to avoid the potential for coverage disputes and costly litigation. The European Commission and EU institutions (including EIOPA), on the other side, could promote and act as an accelerator of this process towards greater transparency and improved mutual understanding.
- **An adequate level and quality of data on cyber incidents need to be available at a European level.** Lack of data is a primary obstacle to a detailed understanding of fundamental aspects of cyber risk and to the provision of proper coverage to the economy. The scarcity of quantitative information on incidents limits the power of quantitative models[9] in making a more proper pricing of risks and estimation of liability exposures and hampers cyber risk measurement and management for insurers. Recently adopted EU regulations, such as the GDPR and NIS Directive, introduced mandatory incident notification frameworks for specific areas, which are expected to produce relevant data. In order to allow for sound pricing, underwriting and cyber risk management, the availability of data on cyber incidents should be broadened and appropriately standardised, while safeguarding the level playing field and data confidentiality. Ultimately, the access to cyber incident database(s), potentially a European Database, could be seen as a public good and underpin the further development of the European cyber insurance industry and act as an enabler of the digital economy.

5. STRATEGY

This section outlines the strategy for EIOPA to achieve the objectives outlined above.

EIOPA's own supervisory and regulatory priorities

Appropriate cyber underwriting and cyber risk management practices and how its supervision needs to be in place to promote such good practices:

- EIOPA to periodically assess cyber underwriting and risk management practices and supervision thereof to address supervisory concerns and foster supervisory convergence, for instance as part of a thematic review on cyber coverages.
- EIOPA to investigate in particular the issue of non-affirmative cyber exposures and potential accumulation risk, with an aim to provide guidance on solution-oriented and mitigating actions on treatment of non-affirmative cyber risk, sound underwriting practices and accumulation risk.
- EIOPA to engage with the industry and European Commission to investigate cyber underwriting as a separate line of business to provide further clarity

7 See for instance 'Is Cyber Risk Systemic' (AIG, 2017), Could a cyber attack cause a systemic impact in the financial sector? (BoE, Quarterly Bulleting Q4 2018), Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance (Carnegie Endowment for International Peace, 2018), Cyber Insurance and Systemic Market Risk (EastWest Institute, 2019), The Ties That Bind: A Framework to Assess the Linkage between Cyber Risks and Financial Stability (SIPA, 2018). ESRB report on Systemic Cyber Risk (forthcoming)

8 Among others, the OECD (2017), the Geneva Association (2018), the Carnegie Endowment for International Peace (2018), the EastWest Institute (2019) and EIOPA (2019) have all called for exploring backstops for systemic cyber risk.

9 Evidence shows that qualitative models are more frequently used than quantitative models to estimate pricing, risk exposures and risk accumulations in the context of the cyber insurance European market. See EIOPA(2018) "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies"

on the coverage provided and allow for better risk assessment.[10] This could also be a starting point as a follow up to the ENISA (2017) recommendation to create minimum coverage requirements per type of coverage on top of which insurers can build extra coverage.

- EIOPA to start collecting information on cyber underwriting and make it available to the public, making cyber an area addressed regularly in EIOPA Reports. Amendments are currently proposed for reporting on cyber underwriting as part of the Solvency II Reporting Review.

Adequate assessment and mitigation tools to address potential systemic cyber and extreme risks:

- EIOPA to include cyber risk events and cyber incident scenarios in its stress testing framework to assess potential vulnerabilities/losses to cyber risk in underwriting. This could be developed for future EIOPA stress test exercises in consultation with external data providers/cyber risk analytics companies.
- EIOPA to incorporate cyber risks within its Risk Dashboard framework.

EIOPA's role as a facilitator and catalyst with the aim to advice on cyber insurance

A mutual understanding of contractual conditions and terms, for both, policyholders and insurance undertakings:

- EIOPA to continue organising workshops to promote on-going dialogue between industry and consumers and to engage with different stakeholders as needed (e.g. FERMA) to promote a more active dialogue with the industry. This should support a better understanding of potentially diverging underwriting practices, raise awareness on cyber security for the demand side, identify areas for improvement and promote good practices in providing cyber coverages, in line with the ENISA findings and recommendations for cyber insurance (2016[11] and 2017).
- EIOPA to continue to monitor market developments and promote good practices if needed from a consumer protection perspective. Such areas could for instance include the transparency of coverages, exceptions for "cyber warfare" and/or distinctions between malicious/non-malicious coverages.

Adequate assessment and mitigation tools to address potential systemic cyber and extreme risks:

- EIOPA to assess and monitor the extent of potential systemic cyber risks and explore the need for systemic mitigants together with the industry, European Commission, the ESRB and other relevant regulatory bodies for potential systemic cyber events, depending on the extent of the systemic cyber risk (based on for instance the outcome of the EIOPA Sress Test and/or other analysis – for instance by the ESRB). Further research is desirable to explore, when applicable, the possible solutions to address potential systemic cyber risks and to evaluate the potential for aligning extreme event risk sharing platforms across perils (nat-cat, cyber and/or terrorism).
- Finally, EIOPA will continue to participate in the EU-US dialogue on cyber insurance to foster knowledge exchange on cyber underwriting (main challenges and good practices, the role of reinsurers and potential systemic cyber risk.)

An adequate level and quality of data on cyber incidents need to be available at a European level:

- EIOPA to engage with its Members, the European Commission and other relevant regulatory bodies (such as ENISA, European Data Protection Supervisors, IAIS) to explore and promote the development of a harmonised cyber incident reporting taxonomy to underpin cyber underwriting modelling. This work can leverage on already existing taxonomies, with an aim to promote the development of a centralised (anonymised) database on cyber incidents, to foster data sharing. EIOPA would act as a facilitator and advisor in this regard, by providing input to policymakers and other regulatory bodies, for instance by contributing to a future NIS Directive Review, in particular when it comes to cyber incident reporting of

10 In the US, the NAIC currently has the following designation for Cyber Liability under Other Liability: "Stand-alone comprehensive coverage for liability arising out of claims related to unauthorized access to or use of personally identifiable or sensitive information due to events including but not limited to viruses, malicious attacks or system errors or omissions. This coverage could also include expense coverage for business interruption, breach management and/or mitigation services. When cyber liability is provided as an endorsement or as part of a multi-peril policy, as opposed to a stand-alone policy, use the appropriate sub-type of insurance of the product to which the coverage will be attached."

11 Cyber Insurance: Recent Advances, Good Practices and Challenges (ENISA, 2016)

Digital Service Providers (DSPs) and Operators of Essential Services (OESs).[12] These European initiatives for a cyber-incident reporting taxonomy could potentially also form the basis for a global taxonomy.[13]

- As part of exploratory work on a potential harmonised cyber incident reporting taxonomy, EIOPA would engage with the industry to better understand their perspective on the minimum standards such a potential cyber incident reporting taxonomy should have to be usable for underwriting and risk management purposes. In this area the market is already developing some initiatives on the area of cyber incident taxonomies[14] and data availability.[15]
- Furthermore, EIOPA would encourage data and knowledge sharing initiatives among industry participants on cyber incidents.

12 In May 2021, 3 years after the transposition of the NIS Directive, a holistic Commission review will take place.

13 At the same time, as part of the work on cyber resilience of insurance undertakings, a properly structured and appropriate Incident Reporting Framework for the financial sector needs to be addressed, together with the other ESAs. Such a framework should be coherent among Europe and kept as simple and flexible as possible in order to avoid creating too much burden on reporting subjects and allow for the dynamic nature of cyber incidents.

14 For instance through the CRO Forum - Concept Paper on a proposed categorisation methodology for cyber risk (CRO Forum, 2016), Insurance Europe - GDPR Data Breach Notification Template (Insurance Europe), Lloyd's Cyber Core Data requirements and the Cambridge Centre for Risk and Studies Cyber Insurance Exposure Data Schema.

15 For example through specialist cyber analytics companies, such as Advisen, CyberCube and Verisk/AIR.

LEARN MORE

Visit the dedicated webpage:

https://www.eiopa.europa.eu/browse/innovation_en

CONTACT US

Westhafenplatz 1,
60327 Frankfurt am Main, Germany
https://www.eiopa.europa.eu/

PDF ISBN 978-92-9473-225-5 doi: 10.2854/793935 EI-03-20-037-EN-N