SUPERVISORY STATEMENT ON THE MANAGEMENT OF NON-AFFIRMATIVE CYBER EXPOSURES

EIOPA-BoS-22-414
22 September 2022

European Insurance and
Occupational Pensions Authority

1. LEGAL BASIS

1.1 The European Insurance and Occupational Pensions Authority (EIOPA) provides this Supervisory Statement on the basis of Article 29(2) of Regulation (EU) No 1094/2010[1]. This Article mandates EIOPA to play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union.

1.2 EIOPA delivers this Supervisory Statement on the basis of Article 44(1), Article 45(1) and (2), and Articles 183 to 186 of the Directive 2009/138/EC (Solvency II)[2].

1.3 This Supervisory Statement is addressed to the competent authorities, as defined in Article 4(2) of Regulation (EU) No 1094/2010[3].

1.4 The Board of Supervisors has adopted this Supervisory Statement in accordance with Article 2(7) of its Rules of Procedure[4]).

2. CONTEXT AND OBJECTIVE

1.5 The frequency and sophistication of cyber incidents in the financial sector, but also to non-financial entities, has increased substantially[5] over the course of the last few years, as economic and financial activities have been heavily digitalised. More recently, the Covid-19 pandemic has been an accelerator of reliance on digital infrastructures which makes companies, financial entities and consumers increasingly exposed to cyber-related incidents.[6]

1.6 Furthermore, Russia's invasion of Ukraine and the economic and financial sanctions that Member States have triggered in response are creating an environment of instability where incidents related to cyberspace may occur. In this context, the link with the topic of territorial exclusions is paramount and NCAs should ensure that potential policyholders are not driven into confusion regarding fundamental topics, such as exclusion clauses with

[1] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[2] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (OJ L 335, 17.12.2009, p. 1-155).

[3] Notwithstanding the fact that specific points of this Supervisory Statement describe supervisory expectations for insurance and reinsurance undertakings, they are required to comply with the regulatory and supervisory framework applied by their competent authority based on Union or national law.

[4] Decision adopting the Rules of Procedure of EIOPA's Board of Supervisors, available at: https://www.eiopa.europa.eu/sites/default/files/publications/administrative/bos-rules_of_procedure.pdf

[5] As Stakeholders highlight, the grounds of the attacks varies and go across from financial gain, "ecological" attack (disturb non-environmentally friendly companies to operate), theft of the intellectual property, etc. Currently, large companies represent for sure a target for cyber criminals, however with the level of sophistication and potential for higher scale, SMEs may also be targeted due to potential lower levels of security and awareness.

[6] However, as also highlighted by Stakeholders, while Covid-19 accelerated society's reliance on digital infrastructure, with cyber criminals conducting pandemic-related phishing campaigns, it also had a positive effect on the level of cyber awareness across society as a whole.

different scope, target, strategy or application.

1.7 For retail and corporate clients the (re)insurance sector has a key role to play in mitigating the impact of these cyber risks and as such facilitate the transformation of the digital economy and reduce the protection gap. Furthermore, cyber insurance is expected to bring additional benefits, by promoting good risk management practices of policyholders and increasing their cyber awareness[7] and cyber products constitute a small but rapidly expanding class of business in the global insurance market.

1.8 Cyber risk exposures, however, are under increasing scrutiny due to potential ambiguous terms and conditions regarding cyber coverages of some insurance policies[8]. In fact, cyber risk exposures could originate from both affirmative cyber insurance policies or cyber endorsements[9], for which some exclusions may not be clear, and in relation to insurance policies designed without explicitly taking cyber risk into consideration.

1.9 Non-affirmative cyber exposure (also called "silent cyber") refers to instances where cyber coverage is neither explicitly included nor excluded within an insurance policy. If a cyber event materialises, this can lead to potentially significant and unexpected losses across lines of business, ultimately leading to time-consuming, expensive, and unpredictable litigation. As experienced during the pandemic situation with regard to Business interruption claims, denial of claim pay-outs in case of uncertainty in coverage could lead to lengthy court cases which could translate into either significant losses for the sector or to a loss of confidence from policyholders. Uncertainty as to what is covered could also lead to a mis-match between policyholders' expectations about the estimated coverage and actual pay-outs following cyber incidents.

1.10 Similar concerns arise regarding the uncertainty of the qualification of cyber attacks as an act of war and consequently wether it would be included in the general war exclusions. Uncertainties regarding the definition of an act of war, including cyber risks, and the potential identification of the attackers' source from state or government-related agencies, might inhibit the development of robust, socially beneficial cyber insurance markets.

1.11 The difficulty in identifying non-affirmative cyber exposure and coverage is an issue that requires high attention from both undertakings and supervisory authorities.

1.12 The importance and the challenge of supervising cyber insurance risk led EIOPA to issue in 2020 the Strategy on Cyber Underwriting[10]. One of the priorities envisaged in the strategy was to ensure appropriate cyber underwriting and cyber risk management practices and to

[7] In this context, for consumers seeking to increase their resilience, cyber insurance shall be part of the solution. However, risk management should also begin at the level of the entity, and insurers usually expect entities to take control over their exposures and implement some baseline cybersecurity measures as a precondition for purchasing cyber insurance, both for ensuring appropriate coverage and managing exposures.

[8] According to EIOPA's report on Cyber Risk for Insurers – Challenges and Opportunities, "lack of transparency in […] exposures also creates uncertainty for policyholders, as it is often not clear whether their cyber claims would be covered within their insurance policies or not"[8].

[9] Cyber endorsement can be added to general insurances policies to cover specific cyber-related losses.

[10] EIOPA, 2020, EIOPA Strategy on Cyber Underwriting. Cyber underwriting strategy | Eiopa (europa.eu)

establish good supervisory procedures. This Supervisory Statement delivers on EIOPA's strategic priorities for the European cyber insurance market with specific reference to non-affirmative cyber risk[11] and sound management of policy wording and presentation of information, 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.

1.13 Lastly, although this Supervisory Statement does not cover neither overall management of affirmative cyber exposures, nor focuses on management of exclusions only, the link between those areas is structural and inevitable to enhance identification and management of non-affirmative cyber exposures.

3. SUPERVISORY EXPECTATIONS

1.14 Given the context outlined, EIOPA recommends NCAs to dedicate higher attention to the supervision of cyber underwriting risk, in particular to (re)insurance undertakings that have potentially significant exposure to non-affirmative cyber insurance risk and to those who have not yet developed a plan to identify and manage non-affirmative cyber underwriting risk, including tailored considerations regarding the specificities of the multiple Lines of Business and products impacted.

1.15 In particular, considering also challenges to draw a straight line between affirmative and non-affirmative risk, EIOPA recommends to engage in a supervisory dialogue with the undertakings and follow a more holistic and risk based approach in the supervision of at least the following aspects:

a) top-down strategy and appetite for (re)insurance undertakings to underwrite cyber risk;

b) identification and measurement of risks exposure with the purpose of implementing sound cyber underwriting practices, with particular regard to the non-affirmative cyber risk;

c) cyber underwriting risk management and risk mitigation, including the reinsurance strategy.

Top-down strategy and appetite for (re)insurance undertakings to underwrite cyber risk

1.16 NCAs should ensure that, when material, cyber underwriting is included as a key and explicit component of undertaking's overall strategy, which should include risk appetite

[11] Other implication of cyber risks on modelling, reserving, etc are excluded from the scope of this supervisory statement

considerations, both at qualitative and quantitative level (by defining and using appropriate key indicators) .

1.17 NCAs should ensure that the administrative management or supervisory body (AMSB) applies appropriate governance and oversight of the undertaking's strategy towards cyber underwriting and ensure alignment with the undertakings' overall business strategy and risk appetite, also considering the non-affirmative cyber component and defined inclusions or exclusions related to cyber risks.

1.18 Relevant staff[12], including AMSB members, should be sufficiently aware of the risks of non-affirmative and affirmative cyber underwriting, also in case of use of third parties in underwriting processes for which the undertaking retains the ultimate responsibility.

1.19 NCAs should ensure that – subject to a materiality assessment and according to a risk-based approach - (re)insurance undertakings align, monitor, and regularly adjust pricing and capital consideration regarding the overall cyber risk exposure to ensure compliance with undertaking's risk appetite.

1.20 NCAs shall recommend undertakings which have not yet engaged in the process of identifying the potential need for review of the terms and conditions of the contracts regarding their cyber coverage to define a plan and procedures to do so, inclusive of a strategy on how to timely and clearly communicate with policyholders the review of the terms and conditions. This is seen as a priority in case of non-affirmative cyber, assuming that affirmative cyber policies have duly considered these aspects, NCAs shall recommend undertakings to report to supervisors the main findings regarding the process described in this paragraph, to envisage an implementation plan for the review of the terms and conditions, if applicable, and to plan for a prompt and clear communication with policyholders about the extent of their coverage.

1.21 In order to deliver on the above expectations and depending on the materiality of the potential exposure at stake, NCAs should remind (re)insurance undertakings the importance to acquire the needed expertise, for instance by providing adequate training on understanding and managing non-affirmative and affirmative cyber underwriting risk to employees and through strategic recruiting of experienced and skilled cyber underwriting professionals.

Identification and measurement of risks exposure with the purpose of implementing sound cyber underwriting practices, with particular regard to the non-affirmative cyber risk

1.22 NCAs should ensure that (re)insurance undertakings – also engaging adequate resources with multidisciplinary knowledge[13] to support the revision of the terms and conditions

[12] E.g. product development, underwriting, risk management, actuarial function etc.

[13] The multidisciplinary approach of the risk control is a key element. The economical digitalisation has great impact in many areas (property, liability, fraud...).

regarding cyber coverages – promptly identify, manage, and monitor their exposure to potential non-affirmative cyber insurance risk and apply sound cyber underwriting decisions consistent with the overall business strategy set by the AMSB, which includes at the least the following:

a) measuring exposure: specific efforts should be made to deploy risk quantification methods as a means to evaluate potential non-affirmative cyber insurance risk exposure. However, considering the evolving nature of cyber risk, the lack of data on cyber events/losses, and the difficulties in assessing policyholder's exposure to cyber risk, to complement the quantitative assessment, the use of scenario analysis is also encouraged;

b) clarifying coverage: assess the adequacy of the wording in terms and conditions of insurance policies with regards to explicitly including or excluding cyber risks, and amend them if considered adequate. Inclusions and exclusions of cyber risks in insurance policies should be clearly communicated to policyholders, avoiding ambiguity in wording and meaning of products;

c) defining cyber terminology: ensuring that the use of cyber terminology remains consistent across all departments of the (re)insurance undertaking and that mutual understanding of contractual definitions is aligned with internal and external stakeholders, making use of commonly agreed terminology and best practices; and

d) monitoring of exposure: regularly monitoring the cyber threat landscape to be able to identify, classify, and define residual or emerging non-affirmative cyber exposures.[14]

1.23 NCAs should recommend undertakings to devote the needed attention towards traditional war and terrorism exclusions, as they might not take into account the digital reality and might therefore lead to uncertainty and ambiguity regarding coverages. In relation to this, when drafting new terms and conditions undertakings should consider studies and analysis available as well as best practices of the market regarding at least:

a) the assessment of intents and outcomes of cyber events;

b) the characterisation of cyber events as hostile, terrorism or warlike[15] and the related challenges related to these assessments (e.g. identifying the perpetrator or establishing potential links to a state authority).

[14] Regular assessments of risk coverage, exclusions, key benefits and other product-related indicators should be carried out to establish whether these are materially different from what was envisaged during product development; eiopa-pog-statement-july2020.pdf (europa.eu)

[15] See, for example, the Tallinn Manual on the International Law Applicable to Cyber Operations and the Cyber Diplomacy Toolbox developed by the EU ministries of foreign affairs in 2017"

1.24 The outcome of this exercise should lead to terms and conditions that are clear and simple and aligned with the undertaking's overall strategy and cyber risk appetite, while at the same time providing value for money to the policyholder in line with with the target market.

1.25 The pre-contractual information and the advertising material of the cyber insurance product should include the main risks covered and the exclusions that apply in a clear and simple manner to create a unique source and channel of information from product development to distribution and to allow policyholders to make an informed decision when selecting a cyber insurance product or when comparing several options.

1.26 In any case, insurance undertakings should consider that depending on the law applicable to the insurance contract, the burden of proof regarding the existence of the exclusion to the coverage, may often rest with the insurance undertaking.

Cyber underwriting risk management and risk mitigation

1.27 Being aware and understanding the risk is fundamental for appropriate risk management practices and informed decision-making. NCAs should ensure that (re)insurance undertakings develop a comprehensive understanding of potential non-affirmative cyber insurance risk scenarios through the combination of both quantitative (see also Par. 1.23 a)) and qualitative assessments and evaluate and manage their respective exposure, taking into account concentration and accumulation risk.

1.28 NCAs are recommended to ensure that undertakings regularly evaluate and make use of available reinsurance capacity to mitigate accumulation risk related to cyber risks. In the specific case of cyber underwriting, NCAs are recommended to ensure that undertakings assess the opportunity to make use of of reinsurers' capacity to be able to bear large cyber events, through the use of specific reinsurance structures. The possible use of these structures, as appropriately designed also given the specific nature of cyber risks, should be able to cover both affirmative and non-affirmative exposures. On the same line, it is important to monitor the availability of such reinsurance structures and establish a dialogue with reinsurers to identify possible gaps.

1.29 NCAs are recommended to ensure that undertakings support the operational management of cyber risks also through the assessment of the overall solvency needs (Article 45 (1)(a) of Solvency II). Where the undertaking concludes, based on the analysis of its current risk exposure, that it is or could be materially exposed to risks revealed by non-affirmative cyber exposures, this should be reflected in the decision and in the design of scenarios used and documented in the own risk and solvency assessment process.

1. ANNEX I: IMPACT ASSESSMENT

1.1. PROCEDURE AND CONSULTATION OF STAKEHOLDERS

According to Article 29 of Regulation (EU) No 1094/2010, EIOPA should, where appropriate, analyse the potential costs and benefits in the process of issuing opinions or tools and instruments promoting supervisory convergence.

In the preparation of the Supervisory Statement on the management of non-affirmative cyber exposures, EIOPA took into consideration the general objectives of the Directive (EU) 2009/138 (Solvency II) and of the EIOPA Cyber Underwriting Strategy.

The analysis of costs and benefits is undertaken according to EIOPA's Impact Assessment methodology.

1.2. PROBLEM DEFINITION

Policy background

As already highlighted in EIOPA publication "EIOPA Strategy on Cyber Underwriting", non-affirmative cyber exposures remain a source of supervisory concern. While common efforts to assess and address non-affirmative cyber risks are underway, the lack of quantitative approaches, explicit cyber exclusions and action plans to address non-affirmative cyber exposures suggest that insurers are currently not fully aware of the potential exposures to cyber risks. Having clear, comprehensive and common requirements on the governance and management of non-affirmative cyber risks would help to ensure the safe provision of insurance services.

Threat landscape

Cyber-related claims are increasing alongside a growth in the frequency and sophistication of cyber incidents across financial and non-financial sectors. Past incidents like the NotPetya attack have demonstrated the large exposure potential of undertakings to non-affirmative and potentially systemic risk.

Lack of preparedness

Until recently, the broader market has systematically underestimated the volatility of the underlying loss distribution of cyber risks. As indicated by feedback received from the industry, undertakings often lack clear strategies, defined risk appetites and robust methods for quantifying exposures. While awareness is increasing, undertakings lack formalised cyber action plans that also account for non-affirmative cyber risk exposures.

There are significant differences in undertakings' assessments of which policies are likely to trigger non-affirmative cyber risks, leading to potentially significant and unexpected losses and accumulation of losses across lines of business, including long, time-consuming, expensive and unpredictable litigation. According to EIOPA's report on Cyber Risk for Insurers – Challenges and Opportunities, "lack of transparency in […] exposures also creates uncertainty for policyholders, as it is often not clear whether their cyber claims would be covered within their insurance policies or not".

Need for policy action

Consequently, cyber risk coverages are under increasing scrutiny given a frequent lack of clarity and ambiguous terms and conditions regarding cyber coverages of some traditional insurance policies.

The work by EIOPA highlighted to following key areas that need to be clarified:

- Strategy and governance regarding cyber underwriting risk
- Approach taken regarding cyber coverage
- Cyber underwriting risk management

In the absence of coherent policy measures at EU level, the entire industry faces the risk to develop non-homogenous practices and apply them in a non-homogeneous pattern harming the goal of achieving a level playing field with respect to sound cyber underwriting and cyber risk management practices, particularly related to non-affirmative cyber risk exposures.

OBJECTIVE PURSUED

The Supervisory Statement has the following objectives:

- Objective 1: to ensure sound cyber underwriting and cyber risk management practices to mitigate non-affirmative cyber risk exposures;
- Objective 2: to establish good supervisory practices;
- Objective 3: to safeguard financial stability, market integrity and investors' protection.

1.3. POLICY OPTIONS

With the intention to meet the objectives set out in the previous section, EIOPA has analysed different policy options throughout the policy development process.

The following table provides an overview of the most relevant policy issues that have been discussed in the policy development process and the main options considered for each of them. The preferred option for each policy issue is marked in bold.

Policy issue 1: Need for policy action

Policy option 1.1 Introduction of EIOPA Supervisory Statement on non-affirmative cyber risk and cyber insurance exclusions to provide clarity on the management and underwriting of non-affirmative cyber insurance risk

Policy option 1.2 Keep the status quo and not issues any policy actions on the subject

Policy issue 2: Approach

Policy option 2.1: Development of high level principle provisions which are less prescriptive and more flexible

Policy option 2.2: Development of rule-based provisions

The following tables summarise the costs and benefits for the main options considered for stakeholders.

Policy issue 1: Need for policy action		
Option 1.1: Introduction of EIOPA Supervisory Statement on non-affirmative cyber risk and cyber insurance exclusions to provide clarity on the management and underwriting of non-affirmative cyber insurance risk		
Costs	Consumers	Premiums and prices of insurance products may increase, if cyber risks, which were previously non-affirmed, become affirmative within insurance contracts.
	Industry	The application of sound cyber underwriting practices and cyber risk management requirements regarding non-affirmative cyber exposures are expected to lead to one off and some ongoing costs regarding further investments in cyber underwriting expertise, restructuring of existing processes and procedures and staff training. For example, as indicated by stakeholders the cost of a training eintails, on average, 5000 euro per employee, plus costs in terms of time of about 70 hours.
	Supervisors	Some potential costs are envisaged to adequately train staff on non-affirmative cyber insurance risk and develop new supervisory activities related to non-affirmative cyber risk governance supervision.
	Other	N/A

Benefits	Consumers	Successful application of the supervisory expectations creates more clarity and predictability for policyholders regarding their cyber coverages.
	Industry	Ongoing application of the supervisory expectations are likely to lower the overall likelihood to incur significant and unexpected costs caused by cyber incidents.
	Supervisors	Enhanced risk-based supervision. Application of the supervisory expectations are likely to lower accumulation of non-affirmative cyber risk and systemic risk resulting from cyber incidents.
	Other	With regard to the whole (re)insurance sector, sound cyber underwriting and cyber risk management practices of a single undertaking benefits the stability of the sector as a whole.
Option 1.2: Keep the status quo and not issues any policy actions on the subject		
Costs	Consumers	No additional costs are expected
	Industry	No additional direct cost are envisaged. However, given the increase in the frequency and sophistication of cyber incidents, as well as the constantly evolving nature of cyber threats, increasing costs are foreseen to arise in the long-term. Undertakings are likely to suffer potentially significant and unexpected losses and accumulation of losses across lines of business as well as long, time-consuming, expensive and unpredictable litigation.
	Supervisors	Additional costs may arise with regards to the ad-hoc treatment and supervision of non-affirmative cyber risk. Further costs could arise from the accumulation of non-affirmative cyber risk and systemic risk, which may lead to inevitable supervisory intervention (partial cost absorption/ bail outs/ etc.). Supervisory resources might not be used in an optimal way.
	Other	Accumulation of non-affirmative cyber risk and systemic risk is likely to increase across the sector, exposing insurers as well as policyholders to potentially significant and unforeseen costs.
Benefits	Consumers	No material impact as the status quo will be maintained
	Industry	In the long-term no material benefit is expected by maintaining the status quo. In the near-term, undertakings will not need to incur additional direct costs from adaptation of supervisory

		expectations regarding non-affirmative cyber risk management.
	Supervisors	No material impact as the status quo will be maintained
	Other	No material impact as the status quo will be maintained
Policy issue 2: Approach		
Option 2.1: Development of high level principle provisions which are less prescriptive and more flexible		
Costs	Consumers	No material impact
	Industry	Some additional costs may be estimated based on the depth of application of the supervisory expectations. In the long term the cost burden is likely to be reduced in proportion to the initial costs incurred to implement the proposed changes.
	Supervisors	Additional one off and ongoing costs are depending on the depth of supervisory oversight of the proposed changes. Some potential costs are envisaged to adequately train staff on non-affirmative cyber insurance risk and develop new supervisory activities related to non-affirmative cyber risk governance supervision. For example, as indicated by stakeholders the cost of a training eintails, on average, 5000 euro per employee, plus costs in terms of time of about 70 hours.
	Other	N/A
Benefits	Consumers	No material impact
	Industry	Undertakings may find it easier, given greater flexibility and less prescriptiveness, to implement the changes proposed.
	Supervisors	NCAs may find it easier, given greater flexibility and less prescriptiveness, to supervise the changes proposed in a risk-based manner
	Other	N/A
Option 2.2: Development of rule-based provisions		
Costs	Consumers	No material impact
	Industry	Additional costs are envisaged regarding the implementation of the changes proposed. In the long term the cost burden is likely to be reduced in proportion to the initial costs incurred to implement the proposed changes.

	Supervisors	Some potential costs are envisaged to adequately train staff on non-affirmative cyber insurance risk and develop new supervisory activities related to non-affirmative cyber risk governance supervision.
	Other	N/A
Benefits	Consumers	No material impact
	Industry	Undertakings would have a closed set of rules available to comply with
	Supervisors	NCAs would have a closed set of rules available against which compliance can be checked
	Other	Increased consistency in implementation across undertakings

1.4. COMPARISON OF OPTIONS AND CONCLUSION

Policy issue 1

The preferred policy option for this policy issue is 1.1 Introduction of EIOPA Supervisory Statement on non-affirmative cyber risk and cyber insurance exclusions.

EIOPA believes that without the introduction of the additional policy, the current status quo will fail to provide an adequate regulatory and supervisory framework for (re)insurance undertaking and the supervisory authorities in their handling of non-affirmative cyber insurance risk.

Moreover, without the issuance of supervisory expectations at EU level, the entire industry faces the risk to develop non-homogenous practices and apply them in a non-homogeneous pattern harming the goal of achieving a level playing field with respect to sound cyber underwriting and cyber risk management practices.

Finally, given the potentially systemic nature of cyber threats, not issuing proper policy action on the topic could increase the impact of operational risks overall for the entire industry, with potential impacts on undertakings and policyholders.

Policy issue 2

The preferred policy option for this policy issue is 2.1 Development of high level principle provisions on the management of non-affirmative cyber risk and cyber exclusions.

The issuance of more prescriptive rule-based policy action poses the risk of potentially more significant implementation costs for the insurance undertakings as new provisions might not only

require the re-assessment of governance and risk management arrangements in place, but also necessity compliance activities specifically meant to cover non-affirmative cyber risk items.

While rule-based provisions would enable greater consistency in application of the Supervisory Expectations on the management of non-affirmative cyber insurance risk and cyber exclusions, a principles-based approach allows for more proportionality and flexibility, which is also relevant with regards to the changing cyber threat landscape.

EIOPA
Westhafen Tower, Westhafenplatz 1
60327 Frankfurt – Germany
Tel. + 49 69-951119-20
info@eiopa.europa.eu
https://www.eiopa.europa.eu