Response to consultation on EIOPA supervisory statement on management of non-affirmative cyber underwriting exposures

Our reference:	GEN-CYB-22-029	Date:	18-07-2022
Referring to:	Consultation on EIOPA supervisory statement on management of non-affirmative cyber underwriting exposures		
Contact person:	Áine Clarke	E-mail:	Clarke@insuranceeurope.eu
Pages:	9	Transparency Register ID no.:	33213703459-54

Questions to stakeholders

1. *What actions have you already taken to address non-affirmative cyber risk?*

Companies are continually examining their exposure to non-affirmative cyber risk as a key element of their internal risk management process, both to comply with prudential requirements as well as to remain in line with national supervisory recommendations in that regard. In some markets, initiatives are ongoing at association level to examine the coverage provided by cyber policies and compare the policy wording with the intended coverage. In other markets, non-binding model clauses for cyber policies have been developed, where possible, and/or are in the process of being renewed.

- In Germany, non-binding model clauses have been developed to affirmatively exclude or include cyber and blackout events from marine and transport insurance policies.

- In the UK, Lloyd's mandated in 2019 that cyber coverage is either included in, or excluded from, (re)insurance policies. This change was implemented using a phased approach, with the fourth and final stage completed in July 2021. The work of Lloyd's is consistent with the approach taken by the UK's Prudential Regulation Authority, which published a Supervisory Statement in 2017 on the cyber insurance underwriting risk to require Solvency II firms to robustly assess and actively manage their insurance products with specific consideration of non-affirmative cyber risk exposures. Firms are expected to introduce measures that reduce the unintended exposure to this risk through various mechanisms, such as introducing wording exclusions, premium adjustments and cover limits.

- In France, trade association France Assureurs is working on a mapping of the different approaches that companies are taking to address their non-affirmative cyber cover. This follows a press release issued by the French supervisor, the ACPR, in 2019 highlighting areas of improvement for companies in tackling silent cyber risk.

Insurance Europe aisbl
Rue du Champ de Mars 23, B-1050 Brussels
Tel: +32 2 894 30 00
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

2. *What do you consider to be the key challenges and opportunities in addressing and managing non-affirmative cyber risk?*

In term of challenges, addressing and managing non-affirmative cyber risk requires the expertise of dedicated cyber risk engineers. Where fewer resources are available, underwriters must undertake specialised training and certification courses. External vendors offer automated security perimeter evaluations that can help to identify a company's cyber exposure. However all of this training and resources come with significant costs. Additional challenges may arise due to the constantly evolving threat landscape and the need for terminology on cyber risks to be updated accordingly.

In terms of opportunities, addressing, managing and reducing exposure to non-affirmative cyber risk may result in an increase in capacity available to offer affirmative cyber risk coverage. This may present an opportunity for growth in the cyber insurance market, notwithstanding the fact that significant challenges linked to the insurability of the risk are likely to remain (see Q4). In markets in which policies generally do not contain exclusions for cyber risks, reducing non-affirmative cyber risk may lead to a growth in the number of cyber endorsements to traditional policies (property, liability).

3. *Please share your estimates or experiences with costs incurred regarding the training of staff, adjusting procedures and activities regarding the management and governance of non-affirmative cyber risk.*

A cyber training course such as the ISC2 CISSP (Certified Information Systems Security Professional) is estimated to cost €5 000 per employee. This includes the course and exam fees but does not include the hidden cost of preparation time, estimated at around 70 hours.

Adjustment of procedures and activities should occur in different domains: claims (training, proposition, response plan, catastrophe plans), accumulation management (scenario definitions, data acquisition, cyber modelling update), governance and assurance (guidelines, external tools, cyber assessment framework) and risk engineering (technical standard for cyber exposure review, technical standard risk grading for cyber security, cyber self-risk assessment tools). Cost estimation depends on the maturity and size of the company and should be replaced by a list of activities, whether general (claims, accumulation management) or cyber-specific (implementation of a next-generation antivirus, subscription to a security operations centre).

4. *If non-affirmative cyber risk is effectively reduced, do you see capacity/willingness to increase affirmative cyber insurance capacity, based on learnings and/or decreased uncertainty?*

Reducing exposure to non-affirmative cyber risk through a better understanding of the risk may free up capacity in the market for writing affirmative cyber risk. However, challenges linked to the insurability of cyber risk are likely to remain, such as the high accumulation potential and the rate at which the threat landscape is evolving.

5. *Do you currently make use of quantitative and/or qualitative analysis to measure your exposure to non-affirmative cyber risk?*

Qualitative analysis is primarily used to measure exposure to non-affirmative cyber risk, however quantitative risk management methods are evolving. Improving access to quality data would help in further developing quantitative methods of analysis.

- In Germany, the insurance association, the GDV, established a monitoring system for non-affirmative cyber claims to help undertakings to understand and quantify the relevance of non-affirmative cyber risks.

Additional Comments

Please insert here any general comment, if not related to the specific paragraphs and sections above

As a general remark, it is worth noting that while EIOPA has titled its statement "management of non-affirmative cyber exposures", the content of the statement goes beyond this, addressing entities' management of cyber risk as a whole.

Insurance Europe agrees with the approach proposed under Policy Option 2.1 (Development of high-level principle provisions that are less prescriptive and more flexible). High-level guidance on managing non-affirmative cyber exposures should provide the necessary flexibility to the industry to continue adapting underwriting practices to the constantly evolving cyber-threat landscape.

Certain terminology/wording used in the statement would benefit from clarification:

- There is a difference between desired non-affirmative exposures (for instance, in property policies, the cyber-induced fire and explosions, also called inherent silent) and undesired exposures (non-damage business interruption following a cyber attack, also called residual cyber).

- Similarly, under policy options, the paper refers to "accumulation of non-affirmative cyber risk and systemic risk resulting from cyber incidents". Insurance Europe seeks clarity on the wording, as it could be implied that systemic risk emerges from affirmative cyber risk only.

Context and objective

1.5 *The frequency and sophistication of cyber incidents in the financial sector has increased substantially over the course of the last few years, as economic and financial activities have been heavily digitalized. 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*.

The frequency and sophistication of cyber incidents across all sectors has increased substantially, however this is due in large part to the rise of the ransomware as a service (RaaS) business model. While COVID-19 accelerated society's reliance on digital infrastructure, with opportune cyber criminals conducting pandemic-related phishing campaigns, it also had a positive effect on the level of cyber awareness across society as a whole.

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.*

Russia's invasion of Ukraine has most certainly contributed to the environment of instability around the world. However, this environment of instability in cyberspace is not new, nor related specifically to the war, as state-linked cyber criminals from Russia and other countries have been engaged in hostile activity in cyberspace for many years. Furthermore, while industries remain on high alert, the expected steep increase in malicious cyber activity linked to the war has so far not materialised.

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.*

The (re)insurance sector has a role to play in increasing awareness of cyber risk and promoting sound risk management measures among prospective insureds. The sector is part of many initiatives to raise awareness of cyber risks, which is fundamental to increasing resilience. For entities seeking to increase their resilience, cyber insurance can be part of the solution. However, risk management begins at the level of the entity, and insurers usually expect entities to take control over their exposures and implement a checklist of minimum cybersecurity measures as a precondition for purchasing cyber insurance. Cyber insurance should be seen as only one of a range of tools available for retail and corporate clients to use in increasing their cyber resilience, complementing the measures implemented at the level of the entity.

1.8 *Cyber risk exposures, however, are under increasing scrutiny due to potential ambiguous terms and conditions regarding cyber coverages of some insurance policies[1]. In fact, cyber risk exposures could originate from both affirmative cyber insurance policies or cyber endorsements[2], for which some exclusions may not be clear, and in relation to insurance policies designed without explicitly taking cyber risk into consideration.*

Cyber risk exposures are indeed under increased scrutiny due to potentially ambiguous terms and conditions in some policies. However, the sentence beginning "In fact…" should be amended in light of the following points:

- "Affirmative cyber insurance policies" is a redundant term given that, by definition, a cyber policy affirmatively covers cyber risk. The word "affirmative" could be replaced by the word "dedicated".

- The sentence "affirmative cyber insurance policies or cyber endorsements" implies that a cyber endorsement is not an affirmative cyber policy, which is incorrect.

1.9 *Non-affirmative cyber exposure 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.*

Cyber events can lead to potentially significant and unexpected losses in non-affirmative cyber exposures. Therefore, it is vital for undertakings to be aware of those risks and take them into account in risk management and calculation.

Non-affirmative cyber exposures do not necessarily lead to higher uncertainty in claims settlement, and in most cases the opposite is the case. Non-affirmative cyber claims occur when coverage is granted independently of the triggering event (fire, third-party claims, etc.) This is usually easier to determine than the question of whether a specific cyber event triggered the damage.

1.10 *Similar concerns arise with respect to cyber attacks in case they could be qualified as an act of war, as uncertainties regarding the inclusion of such risk in insurance coverage might inhibit the development of robust, socially beneficial cyber insurance markets.*

The treatment of war risk in cyber insurance policies is under increased scrutiny, particularly in light of current events. Discussions are ongoing in some markets to update traditional war exclusions to accommodate war of a cyber nature, for example in France, where the Haut Comité Juridique de la Place Financière de Paris (HCJP) recommended updating the legal definition of war risk to accommodate cyber warfare. Work has also been

[1] According to EIOPA's report 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"

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

carried out by the Geneva Association in the area of attribution, where a new term "hostile cyber activity" has been coined to sit between cyber terrorism and cyber war, with the intention that, going forward, such a term may assist in distinguishing between what is insurable and what is not.

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.*

Undertakings and supervisory authorities should be aware of and pay attention to risks that arise from non-affirmative cyber exposure. However, since there are only a few known cases in Europe of claims covered by non-affirmative cyber coverage, this issue does not require **high** attention, and high-level guidance from EIOPA should be adequate to ensure convergence on this issue across the EU.

1.12 *The importance and the challenge of supervising cyber insurance risk led EIOPA to issue in 2020 the Strategy on Cyber Underwriting[3]. One of the priorities envisaged in the strategy was to ensure appropriate cyber underwriting and cyber risk management practices and to 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[4] 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.*

While the reference to the 2020 work is understandable as a step leading to the present statement, it is worth noting that the awareness of and handling of non-affirmative cyber exposures have strongly increased in the market in the past two years.

Supervisory expectations

1.13 *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.*

No additional comment

1.14 *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.

No additional comment

[3] EIOPA, 2020, EIOPA Strategy on Cyber Underwriting. Cyber underwriting strategy | Eiopa (europa.eu)
[4] Other implication of cyber risks on modelling, reserving, etc are excluded from the scope of this supervisory statement

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

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

No additional comment

1.16 *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.*

No additional comment

1.17 *Relevant staff[5], including AMSB members, should be sufficiently aware of the risks of non-affirmative and affirmative cyber underwriting, also in case of use of consulting services or outsourcing arrangements applicable to business functions (e.g. risk management, distributors, etc.) for which the undertaking retains the ultimate responsibility[6].*

No additional comment

1.18 *NCAs should ensure that (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.*

No additional comment

1.19 *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.*

Given that the EU already operates a comprehensive framework governing the terms and conditions reviews and policyholder communications, this Supervisory Statement should not result in any duplicative requirements, but rather use existing mechanisms.

1.20 *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.*

No additional comment

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

[6] In line with the Solvency II and Delegated Regulation provisions on outsourcing and related EIOPA guidelines

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

1.21 *NCAs should ensure that (re)insurance undertakings – also engaging adequate resources with multidisciplinary knowledge to support the revision of the terms and conditions 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: introducing clear and concise wording in terms and conditions of insurance policies with regards to explicitly including or excluding cyber risks in all policies. 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[7].

The development of common terminology on cyber risks to be shared between (re)insurers, brokers and policyholders is an important area to be explored.

Challenges associated with gathering quality data should also be considered, with assessment questionnaires that are supplied to/received from brokers amended and/or supported by external assessment tools.

1.22 *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 and the related challenges related to these assessments (e.g. identifying the perpetrator or establishing potential links to a state authority).

No additional comment

[7] 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)

1.23 *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.*

No additional comment

1.24 *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 allow consumers to make an informed decision when selecting a cyber insurance product or when comparing several options*.

Paragraph 1.24 relates to dedicated cyber insurance products, however the supervisory statement is aimed at non-affirmative cyber exposures. The point should therefore be deleted.

1.25 *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.*

No additional comment

Cyber underwriting risk management and risk mitigation

1.26 *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. 1.22 a)) and qualitative assessments and evaluate and manage their respective exposure, taking into account concentration and accumulation risk.*

Insurance Europe agrees with the above statement but notes once again the challenge of gathering quality data for quantitative assessments.

1.27 *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 make use of reinsurers' capacity to be able to bear large cyber events, through the use of specific reinsurance structures, such as excess of loss covers or other non-proportional reinsurance arrangements. The 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.*

The supervisory statement should refrain from referring to specific reinsurance structures as examples of the industry, as this might imply that one kind of reinsurance structure is more suitable than another. The reference to "excess of loss covers or other non-proportional reinsurance arrangements" should therefore be deleted. In cyber, the only existing non-proportional covers are stop-loss (or their equivalent aggregate excess-loss).

As regards the last sentence, in general, reinsurers ask that primary insurers only cede affirmative risk, as reinsurance structures are generally not designed to cover non-affirmative exposures.

1.28 *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.*

Insurance Europe would like to point out that the own risk and solvency assessment (ORSA) remains an individual assessment on the part of each company. As such, the incorporation of cyber risks into this analysis should remain at the discretion of the company.