Position Paper

Response to EC consultation on a digital operational resilience framework for financial services

Our reference:	EXCO-CS-20-023		
Referring to:	EC consultation paper on a digital operational resilience framework for financial services		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	15	Transparency Register ID no.:	33213703459-54

General comments:

- Insurance Europe welcomes the efforts to increase the digital operational resilience of the financial sector and recognises the importance of enhancing knowledge sharing and cooperation across the EU.
- Importantly, the quality and value of the content of any Commission's envisaged initiative should be favoured over the speed at which it is introduced. To this end, Insurance Europe stresses the importance of engaging with industry in a fact-finding exercise, in order to identify those areas in which an EU initiative could prove itself to be of added value, given that there are many existing national initiatives (both in the public and private sector) aimed at enhancing cyber and information security.
- While Insurance Europe recognises the need to strengthen the cyber resilience of the financial sector as a whole, it must be stressed that the sector is not uniform. Both the kinds of incidents experienced by different financial services entities, as well as the consequences arising from these incidents, differs greatly from one financial services sector to another. Any European Commission initiative in this area must therefore give due consideration to the specific characteristics of the different types of financial services entities. A one-size-fits-all approach to increasing the cyber resilience of the financial sector will not succeed in its goal.
- Any measures to increase cyber resilience must be proportionate not only to the type, size or financial profile of a relevant entity, but also to the risks they are exposed to and the systems and services that need to be protected and maintained. Insurance Europe stresses the need for a risk-based approach to cyber resilience, distinguishing between critical and less critical functions. The principle of proportionality must therefore be incorporated into any framework which expands obligations for reporting incidents, testing and the exchange of information to all undertakings.
- Insurance Europe welcomes ambitions for a Pan-European approach to operational resilience, however, stresses the importance of alignment between all EU-level regulatory initiatives in this area. We note that the contents of guidelines issued by NCAs or by the ESAs - such as EIOPA's guidelines on outsourcing to cloud service providers and its draft guidelines on ICT security and

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

governance, which are in the consultation phase - overlap greatly with the Commission's initiative on a digital operational resilience framework. Close coordination is therefore essential in order to avoid regulatory overload. Furthermore, interactions between a future regulation on a digital resilience framework and the NIS Directive should be considered and managed in order to avoid inconsistencies and redundancies across regulation applicable to the financial sector.

- The insurance industry has a key role to play in assisting the EU in its efforts to increase cyber resilience, acting as a risk transfer mechanism and providing compensation for losses that cannot be fully prevented. It is therefore a crucial facilitator of the digital transformation. Insurance Europe welcomes the European Commission's recognition of this fact in a section of the consultation devoted to 'cyber insurance and other risk transfer mechanisms.'

ICT and security requirements:

Q1. Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?

- In principle, all financial entities should have in place an ICT and security risk management function based on key common principles, in order to ensure the security of the financial services sector. However, due consideration must be given to the fact that there are significant differences between financial services sectors in terms of their exposure to cyber risks and of the potential consequences of a successful cyber-attack. These differences must be reflected in the envisaged key common principles.
- Any principles must respect the principle of proportionality; the expansion of obligations for reporting incidents, testing and the exchange of information to all undertakings must be in proportion to the size, scale and nature of the undertaking, as well as the risks that the undertaking is exposed to.
- As far as the insurance sector is concerned, ICT risks as a component of operational risks (see Art. 13 No. 33 Solvency II-Directive) are already part of the integrated risk management system of all Solvency II regulated insurers. As such, ICT risks are taken into account in capital requirements, governance and reporting. It is therefore important to ensure that a separate Digital Operational Resilience Framework does not undermine the integrated risk management of insurers nor the principle-based approach and principle of proportionality under Solvency II.
- Alignment between the various EU-level regulatory initiatives in this area is essential in order to avoid double regulation and excessive burden on financial entities (eg. EIOPA consultation on guidelines on ICT security and governance).
- Any risk management approach should, to the greatest extent possible, align with industry standards ISO 27005 (Information security risk management).

Q18. What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)?

- Insurance Europe does not support such an approach, as the complexity of both systems and incidents makes legislating on a specific duration for RTO and references to RPO impossible, regardless of the size of the affected undertaking and regardless of whether the undertaking operates in an infrastructure which has been categorised as 'critical'.

ICT and security incident reporting requirements:

Q20. Is your organisation currently subject to ICT and security incident reporting requirements?

- (Re)insurers in the EU, like all other organisations, are subject to data breach reporting requirements under the GDPR.
- Insurers are not included in the scope of the NIS Directive as Operators of Essential Services (OES). However, a number of Member States have extended the scope of the Directive to include (re)insurers and in these cases, they are subject to incident reporting requirements under the NIS Directive (Germany, France, Portugal, Belgium).

Q21. Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?

- In principle, Insurance Europe sees the merit in improving the reporting of ICT and security incidents as a means of increasing the EU's cybersecurity and enabling the development of the cyber insurance market. 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 with it additional reporting requirements for companies, i.e. on top of the existing reporting requirements in GDPR, NIS Directive, where applicable, 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.
    - Participation must be **voluntary**; however, entities could be given incentives to encourage their participation, which might include access to the anonymised and aggregated data of the other participants, enabling those entities to draw on incident data from across the financial sector to improve their own ICT security (a two-way system). Incident data could also be used by participating companies from the insurance industry for underwriting purposes, encouraging the development of the European cyber insurance market.
    - Incident reporting requirements must be **in proportion** to the size, scale and nature of the undertaking, as well as the risks that the undertaking is exposed to. Operators of critical and less-critical ICT functions must not be subject to the same reporting requirements.
    - Any system of ICT and security incident reporting must be **anonymous**, in order to avoid the reputational issues that may come with the reporting of ICT and security incidents.
    - Any system of incident reporting must align with industry standard reporting frameworks such as Mitre Att&ck, in order to ensure that it is the least disruptive possible for entities that have already in place well-established reporting frameworks and practices.
- Insurance Europe's views on the challenges to cross-border cooperation and information exchange on ICT and security incidents (eg. reporting) can be found in response to Q39.

Q22. If the answer to the previous question (no. 21) is yes, please explain which of the following elements should be harmonised?

- Taxonomy of reportable incidents?
- Reporting templates?
- Reporting timeframe?
- Materiality thresholds?
- Other?

- Consistent with the observations made in response to Q21, harmonisation should be in a way that still guarantees the anonymity of the reporting entity. Any additional reporting requirements must respect existing reporting systems and platforms in place at a national level. The duplication of efforts must be avoided.
    - The establishment of a harmonised system of reporting will require a harmonised taxonomy of reportable incidents, however, Insurance Europe stresses the importance of not 'reinventing the wheel', in this regard. Consideration should be given to existing taxonomies which are used as points of reference by the industry, such as the FSB cyber lexicon.
    - Reporting templates should be harmonised, however they should not be so detailed that they become overly resource-intensive, thus discouraging participation in reporting systems.
    - Any harmonisation of materiality thresholds must not be cross-sectoral, given that cyber-attacks do not affect all financial entities in the same way. See response to Q24.

Q23. What level of detail would be required for the ICT and security incident reporting? Please elaborate on the information you find useful to report on, and what may be considered as unnecessary.

- Information on cyber threats and incidents would be useful to report on, provided that materiality thresholds are implemented.
- Given that the financial sector is constantly the object of minor cyberattacks, with little or no impact, the reporting of these types of minute "incidents" would be unnecessary, given that it would not contribute towards strengthening the cyber resilience of the financial sector.

Q24. Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?

- Materiality thresholds must be implemented, whereby minor incidents would have to be logged and addressed by the entity but would not have to be reported to the competent authority. However, given that cyber-attacks affect different financial entities in different ways, (for ex. a Denial of Service attack might have catastrophic consequences for a bank and its customers but have little consequences for insurers), materiality thresholds should not be uniform across the financial sector.
- In defining materiality thresholds, consideration should be given to definitions in existing requirements:
    - NIS Directive: for an incident to be reported, it must have a material negative impact, according to certain criteria
    - GDPR: for an incident to be reported, it is enough that there is a probability of a negative impact
    - ISO 27000: an information security event is defined as "identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant"
    - ITIL: an incident is defined as "an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a Configuration Item that has not yet impacted an IT service"
- It is worth noting that the variety of existing definitions in place when it comes to materiality thresholds and parameters for ICT and security incident reporting reflects the diversity of actors

(in terms of both criticality and business models), and the variety of existing practises. Once again, this is a reflection of the fact that no one set of materiality thresholds will work for all actors.

- Any planned reporting must not exceed the granularity of reporting systems currently existing at national level (eg. LKRZV in Germany). See response to Q39.

Q25. Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported, or should there be one single authority acting as an EU central hub/database?

- Any rules determining national competent authorities should avoid being overly prescriptive, given that supervision is an area which is largely the responsibility of Member States. The selection of national competent authorities must therefore be at the discretion of Member States.
- The idea of one single authority makes sense, given that cyber-attacks do not respect national boundary lines. However, such an initiative comes up against the challenges posed by language differences and trust issues, among others (see response to Q39). Under these conditions, security incidents could be reported to the national competent authority which would be responsible for the notification of these incidents at a European level.
- The implementation of the NIS directive at European and national level provides a template for such reporting governance. Having said that, Insurance Europe highlights that a blanket extension of incident reporting beyond operators of essential services providers would not be consistent with the approach suggested in Q21 (voluntary, proportionate, anonymised, based on market standards).
- Due attention must be paid to the risks associated with storing information on all security incidents in one centralised database, which would undoubtedly become an attractive target for cyber-attacks.

Question 26. Should a standing mechanism to exchange incident reports among national competent authorities be set up?

- Any such mechanism must align with the considerations laid out in response to Q21. In particular, the anonymity of the incident reports must be guaranteed, and participants must gain access to the incident reports of others.
- Feedback from authorities to financial institutions would be welcomed.

Digital operational resilience testing framework:

Q29. Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be? (Gap analyses? Compliance reviews? Vulnerability scans? Physical security reviews? Source code reviews?)

- While Insurance Europe acknowledges the important role that testing of ICT systems and tools has to play in identifying weaknesses and increasing cybersecurity, it must be noted that the exposure of different types entities to risks is not uniform. Any means of assessment must therefore be sector specific.

- Penetration tests are generally considered as a best practice but, in a first instance, it could be more appropriate to rely on thorough gap analyses and, only after that, the undertaking could assess if it is worth performing a penetration test on risk-based grounds. This should be part of a pluri-annual testing cycle appropriate to the criticality of the ICT systems.
- Baseline testing/assessment of ICT systems and tools must be carried out on a voluntary basis, in accordance with current existing national principles. The results of any testing exercises must be kept confidential.

Q30. For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of a combination of criteria, such as:

Proportionality–related factors (i.e. size, type, profile, business model)?
Impact – related factor (criticality of services provided)?
Financial stability concerns (Systemic importance for the EU)?

-
- It does not appear necessary to create a new loosely defined category for "significant financial entities" given that European Union legislation already provides for more advanced testing for operators of essential services. The concept of operators of essential services is now well known and being implemented at national level and it would be unwise to blur the lines with a new category whose boundaries would spark lengthy discussions. Adjusting foundational ICT and security rules applicable to all entities to sectors' specificities, while providing for more cross-sectoral rules for operator of essential services, is deemed a proportionate approach.

Q31. In case of more advanced testing (e.g. TLPT), should the following apply?

- Should it be run on all functions?
- Should it be focused on live production systems?
- To deal with the issue of concentration of expertise in case of testing experts, should financial entities employ their own (internal) experts that are operationally independent in respect of the tested functions? Should testers be certified, based on recognised international standards?
- Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be held valid for EU regulatory purposes)?
- Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model? Should the ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing guidelines, ensuring coordination)? Do you see a role for other EU bodies such as the ECB/SSM, ENISA or ESRB?
- Should more advanced testing (e.g. threat led penetration testing) be compulsory?

- Any industry-wide initiative in this field should respect the principle of proportionality and should follow a risk-based approach.
- Participation in advanced testing such as threat led penetration testing (TLPT) should be optional, given the likely economic burden such forms of testing can place on companies (80.000-100.000 Euro). See response to Q29.

Q32. What would be the most efficient frequency of running such more advanced testing given their time and resource implications? (Every six months, Every year, Once every three years, Other)

- Given the wide variety of entities active in the financial services area, it does not seem possible to identify a frequency of running more advanced testing that would apply uniformly across the financial sector.
- Rather than specifying a particular frequency, regular advanced testing cycle must fit with the criticality of the ICT systems. If a frequency were to be defined, it remains questionable whether the proportionality of these tests could be guaranteed, as conducting a penetration test on an annual basis would be highly demanding for any undertaking and would conflict with the market practice of pluri-annual planning.
- If general rules governing frequency are to be defined, they should not result in entities, with advanced systems already in place, having to adapt to overly prescriptive but less secure testing systems. It should be noted in this respect that some (larger and more sophisticated) entities are moving increasingly towards continuous testing.

Question 33. The updates that financial entities make based on the results of the digital operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability. Which of the following elements could have a prudential impact?

The baseline testing/assessment tools (Gap analyses? Compliance reviews? Vulnerability scans? Physical security reviews? Source code reviews?)
More advanced testing (e.g. TLPT)?

- Both the baseline testing/assessment tools and more advanced testing would lead to unnecessary and burdensome testing requirements. These would be resource-intensive exercises, which might not positively contribute to overall financial stability.

Addressing third party risk: Oversight of third-party providers (including outsourcing):

Q34. What are the most prominent categories of ICT third party providers which your organisation uses?

- The most prominent category of ICT third party providers used by insurance companies is cloud service providers, which can be divided into many categories, including Private Cloud vs Public Cloud, Multi-Cloud vs Hybrid-Cloud, IAAS vs PAAS. In recognition of this, in January 2020, EIOPA adopted guidelines on outsourcing to cloud service providers.

Q36. As part of the Commission's work on Standard Contractual Clauses for cloud arrangements with financial sector entities, which outsourcing requirements best lend themselves for standardisation in voluntary contract clauses between financial entities and ICT third party service providers (e.g. cloud)?

- Insurance Europe welcomes the planned approach of the Commission to encourage and facilitate the development of standard contractual clauses for cloud outsourcing by financial institutions. The development of such model clauses would allow insurance companies to better reflect their sectoral regulatory constraints, eg Solvency II, in their contractual agreements with cloud service providers. It would also allow for a more consistent approach to such agreements at EU level.
- The focus of the development of any standard clauses should be to help provide the necessary clarity or elaboration to give effect to the requirements set out in outsourcing guidelines and to

ensure that relevant obligations are appropriately reflected in outsourcing arrangements. This is particularly important to avoid any potential imbalance of the negotiating power between insurers and cloud service providers. Areas where this could be particularly useful include access and audit rights, sub-outsourcing, information security and termination/continuity arrangements.

Q37. What is your view on the possibility to introduce an oversight framework for ICT third party providers?

- Insurance Europe agrees that there is a need to ensure that ICT third party providers comply with appropriate ICT and security standards. In this regard, ensuring appropriate oversight is to be welcomed, given that the enforcement capabilities of individual insurers (regarding contractual requirements, audit, monitoring and oversight) are limited. Currently, all of the burden of compliance with the regulatory framework (eg Solvency II) is borne by the insurer. In the event that such a framework is developed, it should set out criteria for identifying the critical nature of the ICT third party providers, define the extent of the activities that are subject to the framework and designate the authority responsible to carry out the oversight. Certification of ICT third party providers could be an element of such an oversight framework.
- We do not believe that financial prudential authorities should be directly responsible for the oversight of critical third-party providers, as their capabilities, resources, expertise and staff have not -by design- been tailored to carry out such a task. Furthermore, any oversight framework should be cross-sectoral (insurers, banks, asset managers, market infrastructure operators all using the same providers and range of products), as should be the body responsible for enforcing it. An extension of the remit of existing authorities such as ENISA or BEREC, or a new focused Authority, may be more appropriate. Prudential authorities could then refer to this body when seeking reassurance on key issues concerning the financial entities under their supervision.
- In this respect, we also welcome the work being done by the European Commission on the development of standard clauses for cloud computing and believe that this is a mechanism through which the ESAs could ensure cloud providers respect the requirements set out in the respective guidelines on outsourcing faced by industry.

Q38. What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers?

- We oppose the proposal to establish a settled rotation for the use of cloud providers, as it is both too costly and too time-consuming for undertakings. Negotiating cloud service contracts often takes months to years until a final agreement can be reached. Furthermore, we question whether this would have any added value, as the transfer of data and starting negotiations from base every time can increase the risk of relevant incidents and be overly burdensome.
- We oppose the idea that limits should be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers, given that it is partially unfeasible e.g. for certain SAAS solutions where there are no alternatives on the market. Furthermore, it would be a massive intervention in the free economic decision-making of every undertaking and would contradict the free flow of non-personal data in the European Union, a key building block of the Digital Single Market in Europe and considered the most important factor for the data economy.
- Concentration risk can be better addressed by:
    - **Regulating cloud services providers** with a body of ICT security, conduct and fair competitions rules and enabling effective supervision by guaranteeing that foreign-based providers can be held accountable in the EU and subject to effective enforcement actions;

- **Fostering standardisation and interoperability** of technical solutions and processes (e.g. containers) allowing a seamless portability of data and applications from a cloud provider to another would naturally increase market discipline among them and facilitate multi-cloud approach and/or exit strategies;
- **Allowing diversification of risks** globally by removing data localisation rules whenever possible.

Information sharing and promotion of cyber insurance and other risk transfer schemes:

Q39. Do you agree that the EU should have a role in supporting and promoting the exchange of information between financial institutions?

- Insurance Europe is in favour of more information sharing across different jurisdictions within the EU. Given the cross-border nature of cyber incidents, the EU has a role to play in supporting and promoting the exchange of information between financial institutions. However, for any platform of information-exchange to work in practise, the kind of information shared should be restricted to the reporting of cyber threats and incidents (see response to Qs on ICT and security incident reporting requirements). Beyond contributing to increasing entities' own cyber resilience, shared data on the above, once anonymised and aggregated, could be used by the insurance industry for underwriting purposes. This would encourage the further development of the European cyber insurance market, thus contributing to Europe's cyber security

- However, the challenges stemming from information sharing initiatives must be stressed:
  - The **degree of fragmentation** of both information collecting and information sharing practises across the European financial sector represents one of the greatest challenges.
  - There can be **reputational issues** for a firm associated with the sharing of information on cyber threats and incidents since it could affect an entity's relationship both with its supervisor and with its peers. An ideal information sharing framework is therefore one which maximises the chances of all participants being willing to share information so that, in participating, no one entity risks more than another. Such an arrangement is therefore conditional on:
    (i) entities' ability to share such sensitive information with supervisors and peers without fear of consequences;
    (ii) those involved in such an arrangement must trust that the information they share will not be misused;
    (iii) entities must reap benefits from participation in such an arrangement. Feedback/reciprocity is therefore essential, whether participants get access to anonymised and aggregated data in return for their participation, or otherwise.
  - The **lack of a common taxonomy** on cyber risks represents another challenge associated with the cross-border sharing of information on cyber threats and incidents. See response to Q45.2.
  - There are **competition issues** related to information sharing. Not all information is suited to sharing, in particular, data that is commercially sensitive.

Question 43. Does your organisation currently have a form of cyber insurance or risk transfer policy?

- Not relevant for the industry to give a response.

Question 43.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 43 (and its possible sub-question):

- Insurers have a key role to play in increasing cyber resilience, not only by providing risk transfer or cyber cover, but also in helping their clients prevent cyber risks and mitigate their impact when they materialise. Insurers have a unique perspective that goes beyond their experience of cyber risks, thanks to their many years of insuring other similarly large and complex risks, such as natural catastrophes.

- Cyber risk management usually involves methods of reducing the risk of serious consequences. These methods (firewall, intrusion detection, etc.) reduce the risks but do not eliminate them, so the question arises of how to handle the residual risk. One of the tools to manage this residual risk can certainly be to purchase a cyber insurance policy.

Question 44. What types of cyber insurance or risk transfer products would your organisation buy or see a need for?
To the extent you deem it necessary, please specify and explain whether they should cover rather first or third-party liability or a combination of both:

- Cyber insurance can cover a range of damages, for example accidental damage or destruction of software (first party). Some insurers also offer coverage that relates to the privacy, confidentiality and security of data (third-party). Cyber insurance products can therefore cover a combination of both first and third-party liability.
- On top of damage coverage, insurers also offer a range of other services, such as helping clients to identify vulnerable business functions and practises so that incidents can be prevented. In the wake of an incident, insurers offer services that provide their customers with assistance following a cyber security incident, in order to mitigate the adverse consequences. This can include both forensic IT services and legal support. The type of cyber cover available depends to a large extent on national circumstances/specifies, given that the form of an insurance product is closely linked to the specific frameworks in place at a national level (from a legal and a liability point of view). As such, cyber insurance is tailored to the needs of the client and the specific environment in which they operate.

Question 45. Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?

	Yes	No	Don't know /no opinion /not relevant
Lack of a common taxonomy on cyber incidents			Don't know
Lack of available data on cyber incidents	X		
Lack of awareness on the importance of cyber/ICT security	X		
Difficulties in estimating pricing or risk exposures	X		

	Yes	No	Don't know /no opinion /not relevant
Legal uncertainties around the contractual terms and coverage	X		
Other (please specify)	X		

Question 45.1 Is there any other area for which you would see challenges in the development of an EU cyber insurance/risk transfer market?
Please specify which one(s) and explain your reasoning:

- There are still several hurdles that need to be overcome before cyber insurance becomes a mainstream product. One of those is the fact that cyber risks are difficult to quantify and assess, largely due to a lack of good quality data.
- It is particularly challenging to estimate the possible losses stemming from cyber incidents, which can be very complicated. This is due to a number of factors including:
  - uncertainty of potential future losses;
  - highly correlated risks due to widespread use of certain operating systems;
  - multiple (affirmative and/or non-affirmative) guarantees may be triggered in different lines of business;
  - a lack of available data on cyber incidents and losses;
  - increasingly intangible losses.
- In addition, risk awareness-raising is necessary, both in private areas (among EU citizens) and at corporate level (especially among small and medium enterprises) in order to encourage the development of the cyber insurance market and to progressively evolve towards a model of fully affirmative policy guarantees.

Question 45.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 45, by also specifying to the extent possible how such issues or lacks could be addressed:

- **Lack of a common taxonomy on cyber incidents** – Although there is no common EU taxonomy on cyber incidents, there are several taxonomies that have recently been developed and that the industry refers to (FSB cyber lexicon, CFO forum). However, there is evidence that terms rapidly become out of date and evolve to include a much wider scope and definition, given the evolving nature of cyber risk. As such, any fixed taxonomy for reporting risks quickly becoming meaningless. Therefore, while we see the lack of a common taxonomy as a potential challenge to the development of a cyber insurance market, we do not regard an initiative towards a common taxonomy as a priority. In any event, such an initiative would have to leverage on existing resources.

- **Lack of available data on cyber incidents** – there is not yet an adequate level or quality of data on cyber incidents available at European level, due to the fact the European cyber insurance market is still developing. However, in certain markets insurers' have already made serious efforts to build up data. But, as a first step in increasing the volume of data available for cyber underwriting at European level, Insurance Europe is in favour of 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, 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 welcomes active engagement with ENISA on the subject of data-sharing.

- **Lack of awareness on the importance of cyber/ICT security** – There is a lack of awareness among businesses, particularly SMEs, of the cyber risks they are exposed to. Providing training to management and operational teams in information system security would be a first step in overcoming this challenge. Having such training programmes in place may also assist businesses when purchasing cyber insurance, given that it is an important indicator of the level of development of cybersecurity risk management.

- **Difficulties in estimating pricing or risk exposures** – Given that the cyber insurance market is still an emerging market, there is less historical data to analyse in order to estimate pricing and risk exposures. Although this is a challenge, it will become easier as the market develops. This can be facilitated by allowing insurers to access data, not only on threats and incidents, but also on near misses, as outlined above.

- **Legal uncertainties around the contractual terms and coverage** – The exclusion for war or terrorism that may exist in traditional P&C policies can raise legal questions as to their concrete application in case of cyber events. Achieving a workable definition of cyber-war/cyber-terrorism that would provide clarity across lines of business would be desirable, albeit challenging. Furthermore, there is a diverse range of practises and a lack of legal certainty, both within the EU and globally, about the lawfulness of covering the payment of fines (GDPR) or of ransoms after a ransomware attack.

- **Other –** One of the biggest challenges for insurers is to control the accumulation of cyber risk and to manage their commitments concerning cyber coverages offered to their clients. In this regard, insurers must manage the following challenges:

    - The acceleration of digitalisation of both the economy and interpersonal exchanges increases the surface area of computer attacks.
    - The globalisation of the economy leads to vertical (parent company, subsidiary, branch) and horizontal (supply chain) interdependence of the information systems of different economic players.
    - The concentration of IT manufacturers and service providers generates a multiplication of the same hardware and software throughout the world.
    - The development of the cloud by very few players multiplies the problem of data concentration.
    - The diversity of attackers (States, Mafia, Competitors, Hacktivists, Employees, Opportunists) and means of attack (easily accessible on the Darkweb) multiplies exponentially the number of attacks.
    - Their silent covers; the accumulation of cover for the same cyber event by several insurance policies (silent covers / non-affirmative cover) increases the maximum possible commitment of insurers and therefore reinsurers

Question 46. Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area?

Yes

Question 46.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 46 (and possible sub-questions):

- Support in the development of a cyber insurance market is in principle welcome, however, since cyber risks evolve very quickly and continuously it is important to allow insurers the possibility to develop coverage that matches the changing landscape of risks and consumer demands. Insurers need flexibility to tailor policies to their clients' risks and needs, and policy language is still evolving to reflect a constantly changing threat environment.
- Insurance Europe believes that the EU could support the development of EU or national initiatives in the area of awareness-raising, given that a lack of understanding of the importance of cybersecurity, particularly among SMEs, can lead to the absence of adequate measures to ensure cyber resilience. The EU could play a role by supporting the development and provision of cybersecurity training programmes for businesses. This could be done by leveraging on existing initiatives and public-private partnerships at a national level. An overview of these initiatives can be found in Insurance Europe's 2019 publication, Insurers' role in EU cyber resilience.[1]

Interaction with NIS Directive:

Q47. Does your organisation fall under the scope of application of the NIS Directive (i.e. is identified as operator of essential services) as transposed in your Member State?

- Re(insurance) companies in Member States where they have been classified as OES fall under the scope of the NIS Directive.

Potential impacts:

Q57. To the extent possible and based on the information provided for in the different building blocks above, which possible impacts and effects (i.e. economic, social, corporate, business development perspective etc.) could you foresee, both in the short and the long term?

-
- There are numerous benefits associated with developing best practices and standards in terms of risk mapping, threat-related protocols and ICT management, as well as huge ICT costs for firms implementing them. A way to minimise the costs is to base EU law requirements on best market practices as much as possible in order to avoid inflation of standards, obsolescence of requirements set in hard law, redundancies or even inconsistencies. EU law requirements should be sufficiently principle-based to stay relevant over time and proportionate and risk-based to be efficiently implemented. Furthermore, there should be a sensible balance between sectoral rules which are adjusted to be proportionate to the nature/size/complexity of the entities in this sector and cross-sectoral rules that are more appropriate for operators of essential services. Finally, a way to minimise costs would be to enhance the coordination of EU regulatory initiatives (e.g. EIOPA ICT Guidelines are set to apply before the publication of the EU digital resilience strategy, and not the other way around, as it should be).

[1] https://insuranceeurope.eu/sites/default/files/attachments/National%20examples%20A5.pdf

Q58. Which of the specific measures set out in the building blocks (as detailed above) would bring most benefit and value for your specific organisation and your financial sector?

- Development of best practices and standards in terms of risk mapping, threat-related protocols and ICT management.
- All blocks are important however, crucially, the European Commission should concentrate on areas that cannot be handled through industry initiatives, best practices and standards. This is the case when it comes to a proper direct regulation and oversight of third-party providers. The current status quo in the financial regulation, and particularly in Solvency II, is that all the (operational) risks, burden and compliance costs are on the shoulders of the (re)insurance undertakings, i.e. the clients. This status quo is not sustainable if ICT, security and outsourcing requirements continue to grow and sophisticate, knowing that there is a limit in what individual EU clients can obtain from global foreign-based third-party providers.
- The continuous growth of the cyber insurance market, in a prudent and controlled way, is also critical as even first-in-class practices cannot achieve zero-risk. Evolving progressively towards a model of fully affirmative guarantees, addressing legal uncertainties through industry standards (e.g. cyber warfare) or regulatory clarifications (e.g. payments of ransoms) are future avenues for a mature cyber insurance market.