Position Paper

Position on the review of EU rules on the security of network and information systems (NIS2)

Our reference:	EXCO-CS-21-049	Date:	March 2021
Referring to:	Cybersecurity – review of EU rules on the security of network and information systems		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	4	Transparency Register ID no.:	33213703459-54

Summary

Insurance Europe welcomes the European Commission's proposal for a revised Network and Information Security (NIS2) Directive as part of broader efforts to increase the cybersecurity of the European Union. Extending the scope of the Directive to encompass more sectors that are critical to the EU economy and society is an important step towards both achieving this and implementing the EU's Cybersecurity Strategy for the Digital Decade.

Insurers' operational resilience

As the process of digitalisation continues to advance, the insurance industry, like other sectors, finds itself increasingly confronted with cyber threats. The industry is committed to ensuring that it is resilient in the face of such threats and it is preparing for the financial sector-specific Digital Operational Resilience Act (DORA), which will introduce far-reaching and comprehensive requirements for insurance companies in the areas of information and communication technology (ICT) risk management, incident-reporting, stress-testing and third-party arrangements. Given this, and because one single set of cybersecurity rules offers more effective governance than many separate rules, Insurance Europe welcomes the fact that the insurance industry has not been included in the scope of the proposed NIS2 Directive.

Insurance Europe welcomes the proposal to link the NIS ecosystem with the DORA by way of a consultative process between the national competent authorities overseeing the DORA and NIS single points of contact. Given that cyber threats and incidents do not respect sectoral boundaries, a holistic overview of the landscape of cybersecurity in the EU is essential for strengthening the resilience of the bloc.

Nevertheless, the process of adopting sound, flexible and effective cybersecurity tools and adapting to new cybersecurity governance structures is both complex and time-consuming. In addition to future compliance with the DORA, insurance companies have either adapted or are in the process of adapting to new requirements as a result of supervisory guidelines (EIOPA guidelines on outsourcing to cloud service providers and EIOPA guidelines on ICT security and governance). In order that insurers can plan and implement a phased process of adaptation to these guidelines and to the DORA, it is of the utmost importance that there is absolute clarity

around the legal references applicable to insurance companies. Ensuring that insurers remain outside the scope of NIS2 — both now and in the future — is therefore essential.

Against this backdrop, the insurance industry believes that some aspects of the NIS-DORA relationship could benefit from further clarification in order to ensure legal certainty for all entities that fall within the scope of either legal act. In light of this, Insurance Europe proposes modifying the NIS2 text in the following two areas:

- Article 2.6 (scope)

"*Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, **~~provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive~~**, those provisions of that sector-specific Union legal act shall apply*."

The DORA proposal introduces comprehensive requirements for financial entities in the areas of ICT risk management, incident-reporting, stress-testing and third-party arrangements — requirements that are both more detailed and more extensive than those found under the NIS Directive (and proposed under NIS2), as can be seen in the comparative table in annex to this paper. Furthermore, requirements under the DORA will be further elaborated on in the Level 2 technical standards that will be developed by the European supervisory authorities. These requirements under the DORA, by virtue of the *lex specialis* clause (as referenced in recital 13 NIS2), should fully replace existing cyber risk-management and incident-reporting requirements for insurance companies that currently fall under the scope of the NIS Directive. While this is clearly stated in Article 1.2 of the DORA proposal, Article 2.6 of the NIS2 proposal should be modified accordingly to ensure that there is no legal uncertainty for entities that were designated as operators of essential services (OES) following national enactment of the NIS Directive and that also fall within the scope of the DORA. The reference to equivalence in Article 2.6 NIS2 leaves significant room for uncertainty and many open questions, such as who will be required to assess whether the requirements are "at least equivalent"? The amendment proposed above should remove any legal uncertainty in this regard.

- Article 3 (minimum harmonisation)

"Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, adopt or maintain provisions ensuring a higher level of cybersecurity. ***This clause does not apply to the scope defined under article 2(1) of this Directive."***

The transposition of the NIS Directive did not result in a level playing field for insurance companies across EU member states. Rather, the principle of minimum harmonisation introduced in Article 3 NIS — and maintained in Article 3 NIS2 — paved the way for an uneven application of the Directive for the industry, whereby insurers in three member states (France, Germany and Spain) were identified as OES and, in some cases, subjected to detailed and costly requirements.

In order to ensure that the cybersecurity of European insurers remains harmonised at the level of the DORA alone, the minimum harmonisation clause in Article 3 NIS2 should be further refined, as proposed above. This will provide the necessary legal certainty to insurers by ensuring that member states do not add additional sectors, subsectors or types of entities to Annexes I and II.

Insurers as cyber underwriters

In the area of cybersecurity, the (re)insurance industry occupies a unique position, both as a sector that finds itself increasingly vulnerable to cyberattacks and as a business that can offer protection through a range of cyber insurance products and services. European insurers have a key role to play in the prevention, mitigation and transfer of cyber risk across the EU, offering many cyber insurance services to entities that fall into the categories of OES and digital service providers (DSP) under NIS (and "critical" and "important" entities under the NIS2 proposal).

Access to past cyber-incident data of sufficient quality is vital for the growth of the cyber insurance market, however the data that is publicly available at EU level is currently very limited. In their capacity as cyber underwriters, insurers therefore believe that the exchange of information between authorities and the private sector should be improved. The NIS2 proposal offers an opportunity to foster greater transparency about cyber-related incidents by making anonymised incident data available for use by the cyber (re)insurance underwriting community, thus contributing to increasing the overall cyber resilience of the EU.

Furthermore, the degree and format of incident reporting under NIS differs greatly from country to country, which does not promote a uniform and common understanding of cyber threats and incidents across the EU. In light of this, Insurance Europe welcomes the reference in Article 20.9 of the NIS2 proposal (on reporting obligations) to the possible role of ENISA in issuing technical guidance on the parameters of the information included in the summary report, in order to contribute to the provision of comparable incident information. This is a necessary first step towards more harmonised methods of reporting on cyber incidents in the EU. However, this technical guidance should be a requirement rather than just a possibility and Insurance Europe therefore suggests amending Article 20.9 as follows:

"The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA ~~***may***~~ ***shall*** *issue technical guidance on the parameters of the information included in the summary report."*

In conclusion, Insurance Europe believes that the above amendments to the NIS2 proposal will improve the landscape of incident reporting, further clarify the interaction between NIS2 and the DORA and strengthen the DORA's status as the single overarching set of rules applicable to the financial sector.

Annex

NIS2 REQUIREMENTS	***DORA REQUIREMENTS***
Art. 17 Governance	Art. 4 Governance and organisation
Art. 17.1 Responsibility of the management body	Art. 4.2 Accountability of the management body
Art. 17.2 Training, knowledge, skills of the management body	Art. 4.2.f Training on ICT risks and skills for all relevant staff
	Art. 4.4 Members of the management body shall, on a regular basis, follow specific training
	Art. 5 ICT risk management framework
	Art. 6 ICT systems, protocols and tools
Art. 18 Cybersecurity risk management measures	Art. 7, 8, 9, 10
Art. 18.2 a) Risk analysis and information system security policies;	Art. 7 Identification
(b) Incident handling (prevention, detection, and response to incidents);	Art. 8 Protection and prevention+ Art. 9 Detection
(c) Business continuity and crisis management;	Art. 10.1 and 10.2
(d) Supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services	Chapter V, section I Key principles for a sound management of ICT third party risk Art. 25 General principles Art. 26 Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements Art. 27 Key contractual provisions
(e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Art. 22 Testing of ICT tools and systems (including vulnerability)
(f) Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;	Art. 21 General requirements for the performance of digital operational resilience testing
	Art. 23 Advanced testing of ICT tools, systems and processes based on threat led penetration testing
	Art. 24 Requirements for testers
(g) The use of cryptography and encryption.	Art. 8.4.d Policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys whereby data is encrypted based on results of approved data classification and risk assessment processes; Art. 14.a Future RTS to specify further elements to be included in the ICT security policies, procedures, protocols and tools: including cryptographic techniques
Art. 18.3 To take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	Chapter V, section I Key principles for a sound management of ICT third party risk Art. 25 General principles Art. 26 Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements Art. 27 Key contractual provisions
Art. 18.4 Corrective measures	Art. 4.2.i, Art. 21.1, Art.27.2.d
	Art. 15 ICT-related incident management process
	Art. 16 Classification of ICT-related incidents
Art. 20 Reporting obligations	Art. 17 Reporting of major ICT-related incidents
Art. 26 Cybersecurity information-sharing arrangements	Art. 40 Information-sharing arrangements on cyber threat information and intelligence