Response to EC consultation on the Cyber Resilience Act

Our reference:	EXCO-CS-22-052	Date:	23 January 2023
Referring to:	https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act		
Contact person:	Kenny Piasecki Policy advisor, general insurance	E-mail:	piasecki@insuranceeurope.eu
Pages:	3	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the European Commission's (EC) ambition to raise the level of cybersecurity in the European Union through the introduction of common cybersecurity standards for digital products. The insurance industry's use of digital products will be governed by the forthcoming Digital Operational Resilience Act (DORA). The sector should, therefore, not be included in the scope of any requirements introduced under the Cyber Resilience Act (CRA).

The cybersecurity rules within the Cyber Resilience Act are still needed for those sectors in which they do not exist. However, they should not be so detailed as to constitute a barrier to technological innovation, which is particularly rapid and important in the case of digital products. The rules should also not place EU manufacturers and distributors in an unequal competitive position vis-à-vis operators outside the EU. However, the CRA is an important step towards better management of the risks associated with digital products, which in turn can improve the insurability of the product and the suppliers.

Building on the previous response to the EC consultation on the cybersecurity of digital products and ancillary services, Insurance Europe would like to propose the following comments:

- **Insurers' use of digital products/DORA**

The insurance industry welcomes the general strengthening of cybersecurity across the EU. The Network and Information Security (NIS) Directive (both NIS1 and NIS2) and especially DORA will significantly increase the level of cybersecurity in financial services. In this context, a text that would strengthen the cybersecurity of digital products used by insurers will contribute to the security of the entire ecosystem. For better coherence between the initiatives on cybersecurity at EU level, there should be clarification of the interplay between NIS2, which regulates digital service providers, and the CRA, which will regulate digital products. Nonetheless, the DORA should remain the single overarching set of rules applicable to the insurance industry, and insurers should remain outside the scope of any requirements introduced under the CRA.

In relation to the request for more coherence, Insurance Europe requests further clarity on the scope of the CRA and how it will apply in practice. While the intention is to only include digital products placed on the internal market, there should be an assurance that the scope cannot be interpreted as being wider than that. This is in line with the fact that technology is continuously developing and there must be consideration for how the regulatory framework will continue to fit in. It is uncertain whether current proposals include the necessary level of flexibility to take this into account.

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

- **Alignment and Clarification of definitions**

Insurance Europe welcomes the fact that the proposal is coherent with the current product-related EU regulatory framework, as well as with recent legislative proposals such as the EC's proposal for an Artificial Intelligence (AI) Regulation. **Articles 8** and **41 (10)** provide the link between the CRA and the AI Regulation.

Insurance Europe welcomes the clarification of the definition of importers. The distinction made in **Article 15,** where an importer or distributor shall be considered as a manufacturer when placing a product with digital elements on the market under trademark or with a substantial modification, is sufficient in determining that importers, being vendors, will not also be classified as users.

Insurance Europe asks for clarification of what constitutes a failure. **Article 35 (1)** mentions the seriousness of a failure in reference to the fulfilment of obligations. However, there is no clear definition in the text of what a failure is, and it is uncertain of how seriousness is classified and the consequences of such a failure. A lack of clarity would have an impact on product liability insurance, among other things.

- **Liability**

Insurance Europe welcomes the lack of inclusion of liability regarding security updates, as it was requested to maintain within the realm of the Product Liability Directive. The CRA should not contain specific requirements on the subject, as the liability aspects should be governed by the general liability rules and not by specific rules in the CRA. There needs to be sufficient data available for such governance on general liability rules to be feasible.

- **Certification Schemes**

Insurance Europe welcomes articles which aim to emphasise the interoperability of the European Union Agency for Cybersecurity's (ENISA) certification schemes and the CRA. **Article 6 (5)** sets out that manufacturers shall be required to obtain a European cybersecurity certificate under the Cybersecurity Act to demonstrate conformity as outlined in Annex I of the CRA. In addition, **Article 18 (3)** establishes that products with digital elements that have received an EU statement of conformity or certificate issued under a European cybersecurity certification as specified under the Cybersecurity Act, shall be presumed to be in conformity with essential requirements set out in Annex I of the CRA. In accordance with these articles, the CRA will have to take into account the future cyber certification scheme proposed by ENISA for cloud providers: the European Union Certification Scheme for Cloud Service Providers (EUCS). The interoperability between these different initiatives is a fundamental element that must be considered.

- **CRA and insurance for digital products**

Insurance Europe maintains the position that entities, being users, that cannot demonstrate the ability to manage cyber risks, including ensuring its digital products are secure, will likely have difficulties when attempting to purchase cyber insurance. Although responsibility for managing cyber risks does fall on the user, Insurance Europe welcomes the articles presented in the CRA which aim to provide them with the necessary information and protection to manage such risks. Examples include **Article 10 (2),** which outlines how manufacturers must assess the cybersecurity risks associated with a product with digital elements and prevent security incidents in relation to users, and **Article 10 (10),** which states that manufacturers shall ensure that products with digital elements are accompanied by information and instructions in language easily understood by users, which will allow for a secure installation, operation, and use of the products with digital elements.

Although Insurance Europe welcomes necessary information to help entities manage risks, there needs to be an assessment on the severity of penalties imposed on entities. In particular, **Article 53 (5)** states that the

supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to €5 million or, if the offender is an undertaking, up to 1% of its total worldwide turnover for the preceding financial year, whichever is higher. There is concern for the implication this could have for insurers, particularly when there is the supply of unintentional incorrect or incomplete information. Clarification should be provided so that entities are not penalised without warning or notice when potentially wrong information has been provided.