Key messages on EC consultation on a Cyber Resilience Act

Our reference:	EXCO-CS-22-022	Date:	26-05-2022
Referring to:	EC public consultation on the cybersecurity of digital products and ancillary services		
Contact person:	Áine Clarke	E-mail:	Clarke@insuranceeurope.eu
Pages:	2	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the European Commission's ambition to raise the level of cybersecurity in the European Union through the introduction of common cybersecurity standards for digital products. As society continues to embrace the digital transformation and as the use of digital products becomes more widespread, ensuring that these products are designed to be secure, and can remain so throughout their lifecycle, is increasingly important.

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). However, enhanced cybersecurity requirements are needed for those sectors for which they do not already exist – albeit requirements that are sufficiently principle-based to not become barriers to technological innovation.

Insurers also have a key role to play in contributing to the safety of digital products by offering a variety of insurance solutions (cyber and/or third-party liability) to manufacturers, developers and users of these products. The EC's initiative is an important step towards managing the risks associated with digital products, which, in turn, can improve their insurability.

Insurance Europe would like to propose the following comments in response to the EC's public consultation on the cybersecurity of digital products and ancillary services.

Insurers' use of digital products/DORA

Under the CRA, insurers would fall into the category of users of digital products, according to the definition in the consultation paper. Insurers, like other business industries, make use of a wide range of software and hardware solutions provided by software developers and hardware manufacturers, also known as information and communications technology (ICT) third party service providers.

Insurers' use of the services offered by these providers will be governed by the rules established in the forthcoming DORA. Article 3(16) of the EC's DORA proposal defines ICT services as "digital and data services provided through the ICT systems to one or more internal or external users, including provision of data, data entry, data storage, data processing and reporting services, data monitoring as well as data-based business and decision support services". Before entering into contractual arrangements with ICT third-party service providers regarding the use of their ICT services, as well as throughout the duration of the use of the services, insurers

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

will be required to ensure that their providers adequately manage their cyber risk. In light of this, 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.

Alignment and clarification of definitions

Although the insurance sector's use of digital products should be regulated under DORA alone, the interplay between the CRA and DORA must be clarified given the clear overlap between parties qualifying as vendors under the former and ICT third party service providers under the latter. Here, Insurance Europe calls for consistency in the definitions employed across different areas of EU legislation given that new cybersecurity requirements for digital products will not operate in isolation but in tandem with other EU initiatives in the field of artificial intelligence (AI), data and cybersecurity. In particular, the key categories of vendor and user introduced by the EC under the CRA must be defined in the context of provider and user under the proposed AI Act, as they would appear to encompass many of the same groups and functions. Given the volume of new definitions being proposed particularly in the context of the AI Act – developer, deployer, user, operator, provider, to name but a few – close coordination between those responsible for drafting the various initiatives is essential so that a complicated and contradictory legal landscape can be avoided.

Given the inclusion of importers under the definition of vendor in the consultation paper, a company that imports a digital product from outside the EU for use in the EU, whether for its own use (eg a software solution) or for use by its customers (eg an insurance telematics device), could currently fall into both categories. Users – whether business or consumer – should not qualify as vendors, even if they use a product that is customised, given that they have limited-to-no influence on the actual characteristics (and cybersecurity standards) of the product. Furthermore, key related concepts introduced in the consultation paper, such as what it means to deploy or to distribute a digital product, must also be defined, both in this context and in the context of the other parallel legislative initiatives that are ongoing. This is also relevant for questions of vendors' liability, given the initiatives to revise the Product Liability Directive (PLD) and establish a separate liability regime for 'operators' of high-risk AI; another term that must be defined in this context.

Liability

The liability of vendors is addressed in Question 16 of the consultation paper. However, rules regarding vendors' liability should not be established under the CRA but should be left to the existing framework of liability legislation – the PLD complemented by national tort law. Vendors are considered as producers under the PLD and are therefore held strictly liable for defects arising in their products. Insofar as vendors (producers) should be held liable for a cybersecurity incident resulting from a failure to supply the users of their digital products with the necessary updates, users should assume liability if they fail to apply the updates.

Certification schemes

Insurance Europe strongly supports the introduction of certification schemes, such as those being developed by the European Union Agency for Cybersecurity (ENISA) in the context of the EU Cybersecurity Act, for use by providers to demonstrate fulfilment of and compliance with their rights and obligations under DORA and the CRA. ENISA's certification schemes should be interoperable with these aforementioned legislative initiatives, and a clear link should be established between them.

CRA and insurance for digital products

As previously mentioned, the insurance industry contributes to the safety of digital products by offering insurance coverage. Question 4 of the consultation paper addresses this area and considers whether a user will face additional costs due to highly priced cyber insurance if the digital products it uses are deemed not to be cyber secure. In general, such considerations form part of the exchange that takes place between insurer and insured before cyber insurance coverage is sold. If an entity ("user", in this case) cannot demonstrate that it has taken steps to manage its cyber risk, including ensuring that its digital products are secure, then it is likely to face difficulties when purchasing cyber insurance.