FERMA FOCUS

DIGITALISATION

FERMA

Federation of European Risk Management Associations

FERMA's feedback on the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020, aka 'the Cyber Resilience Act (the CRA)'

23 January 2023

Summary

- FERMA is pleased to provide feedback to the European Commission on the proposed Cyber Resilience Act (the CRA) on behalf of the risk management community.
- While FERMA is, on the whole, supportive of the intention behind the CRA, namely to raise the level of cybersecurity of digital products in the EU (and beyond), we have some practical concerns, which we hope will be addressed by the time the text is finalised.
    - First, on the obligations of manufacturers, importers and distributors, FERMA wants to underline the importance of the *proportionality* of the requirements, as well as the need to ensure *feasibility* of complying with all requirements considering high utilisation of open-source software.
    - Second, on the penalties, FERMA is concerned that the introduction of fines in the context of cybersecurity will lead to a complex landscape of fines according to different pieces of legislation and could also open up (or widen existing) gaps in the insurance coverage of companies.
- FERMA rests at the European Commission's disposal to discuss further the insurance implications of the proposed CRA, as well as the more practical elements related to cybersecurity risks and cybersecurity risk assessments.

The Federation of European Risk Management Associations (FERMA) is a European professional association, which represents, through its 22 Member Associations in 21 countries, nearly 5,000 risk professionals. Risk managers generally have a high level of cooperation with the IT departments in their organisations, as well as with information security teams. When surveyed on the different risks facing companies today, risk managers are highly preoccupied with cyber risks, often citing them as the most pressing concern for their organisations.[1]

FERMA is positive about the CRA. We believe it will raise the bar on cybersecurity in the Single Market through the introduction of legislation on horizontal requirements.

As a community of risk managers we are, however, concerned with two specific parts of the proposed CRA text and its implications. These areas are broadly grouped as the obligations introducedand the proposed penalties. We submit our comments as a contribution to the political discussions and we look forward to an improved final text.

Obligations

As FERMA we are delighted to see prominence given to thorough assessments of cybersecurity risks under the 'Obligations of manufacturers' set out in **Article 10 (2)**. Minimising cybersecurity risks and their impacts is crucial for organisations in protecting themselves against cybercrime.

In reference to **Article 10 (12)**, currently, and based on the experience with the ETSI EN 303 645 standard, the most significant requirement would here be *prior* to the placement of the product on the market. In view of

[1] See more in the FERMA European Risk Manager Report 2022, https://www.ferma.eu/app/uploads/2022/07/ERM-REPORT_FERMA_2022_FINAL.pdf

FERMA's EU Transparency Register identification number: 018778010447-60

the proposed wording in the CRA that each product would have to be evaluated for the period of five years after placing on the market, there also needs to be some sensitivity given to the varying resources of manufacturers. The larger ones will have a less onerous task to continuously monitor and evaluate the cybersecurity of their products than smaller organisations.

This is all notwithstanding the fact that five years in cybersecurity is a long time and standards and norms quickly evolve, as too do the threats themselves. However, as with almost everything related to cyber, and/or digitalisation more broadly, there will be some difficulty in evidencing 100% full compliance at all points in time, since there will always be some degree of 'lag' after, for instance, identifying a vulnerability. It is our view that there might always be a moment where products are somehow temporarily non-compliant at some stage during their lifecycle.

There is some concern from the risk management community about the cost of compliance with the vulnerability management over the lifecycle becoming unmanageable. Currently, most—if not all—software has an open-source component. This open-source component makes it practically impossible to evaluate the entire chain of dependencies and interlinkages for their compliance with cybersecurity standards or levels. In turn, this implies extensive testing for organisations, which might result in increased costs for everybody, from manufacturers, to importers, to consumers.

Penalties

It is important to emphasise that we are generally of the view that cybersecurity would be improved if it were enforceable. Fines are obviously one way to achieve this. However, it is important to ensure that different laws do not duplicate fines, and that there are clear and definite triggers for specific fines. For example, what would happen in the event some compliance with the CRA inadvertently leads to breaches in product liability requirements, or even in GDPR? What takes precedence in instances like this will timportant for companies to know on a practical level.

As alluded to above, there is also some fear about compliance with the CRA when considering the widespread use of open-source software, which is specifically important in the context of **Article 53 (5)**. The use of open-source software can complicate the evaluation of cybersecurity since the chain of dependencies is difficult to fully assess. Furthermore, how can vendors and service providers increase cybersecurity compliance of open-source software while keeping costs at the same or at least a reasonable level? If this cannot be done, there is a residual risk that remains.

A key question here would be whether the insurance market could help transfer that risk. FERMA would like to work with the European Commission further on analysing the possible consequences for insurance coverage that the CRA might have. Right now, for example, when companies purchase a cyber insurance policy there is often—if not always—a product liability exclusion, while when purchasing a product liability policy there is often—if not always—a cyber exclusion. This leads to a gap in protection—and this we believe is something that should be on the Commission's radar in the process of the next steps on the CRA.

About FERMA

The Federation of European Risk Management Associations brings together 22 national risk management associations in 21 European countries. FERMA represents the interests of nearly 5000 risk and insurance managers in Europe active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. More information can be found at www.ferma.eu

FERMA's EU Transparency Register identification number: 018778010447-60