FERMA FOCUS
DIGITALISATION

FERMA
Federation of European Risk Management Associations

FERMA's position paper on the European Commission's Cyber Resilience Act initiative

24 May 2022

Summary

FERMA welcomes the opportunity to contribute to the European Commission's reflections on a proposed initiative on an EU Cyber Resilience Act (CRA).

Cyber risk management is a top priority issue for companies. In fact, it has grown in importance in recent years. For instance, in 2018 when FERMA surveyed European risk managers, 37% of the respondents identified cyber threats as the most critical to their organisation, which rose to 63% in 2022.

FERMA's present position paper is built around two sections:

1. Targeted comments on the CRA; and,
2. More general comments on cyber resilience.

We conclude each section by providing recommendations based on our collective experience and expertise. These comments are provided on behalf of the professional risk management community and we look forward to engaging with the European Commission further on the CRA in coming months.

1. Targeted comments on CRA

It is FERMA's view that the risks **identified** by the European Commission in the context of its CRA initiative are accurate.

Nonetheless, it is our **assessment** as risk managers that the levels of cyber security and cyber resilience in the EU are lower than desired. Many companies (especially **SMEs**) currently have neither the resources nor the knowledge to evaluate the **level of cyber security** of goods and services. Also, there are still gaps in **knowledge and training in cyber security**, more generally.

In this respect, we identify an issue of **education and awareness**:

- There are not enough cybersecurity experts.
- Users of software and hardware are generally not well-enough trained in cybersecurity.

These observations are especially valid for SMEs since they often lack the financial resources of larger companies and generally do not have a dedicated ICT/cybersecurity person. There is also a tendency towards outsourcing made by SMEs. These issues by extension cause problems for large enterprises since there are SMEs in their supply chains.

Moreover, the current identified practices for assessing levels of cybersecurity of products and ancillary services varies across organisations. However, there are some common threads across approaches, which include but are not limited to: certification, audits, insurance, as well as specific terms and clauses in contracts.

Finally, an important observation in this context, is that organisations are regularly confronted with a tradeoff between enabling and protecting business. The more requirements and standards that are

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

placed on suppliers for example make it more difficult for contracting business. So, it is important to find the appropriate balance between these factors in the CRA initiative.

Overall, it is FERMA's assessment that an initiative at EU level that would seek to harmonize practices and provide clear benchmarks on cyber security could be significant.

Therefore, FERMA recommends the following considerations for a CRA initiative:

- A **Horizontal legislation for the CRA** involving the implementation of a common regulatory approach applicable to all categories and risk profiles of ICT products should be considered to guarantee the functioning and harmonisation of the Internal Market, a certain level playing field and the development of the Digital Single Market. Within this horizontal legislation an important goal would be to achieve a **common legal basis** defining:
  - mandatory requirements,
  - certification processes,
  - risk assessment models; and,
  - post market surveillance mechanisms.
- It is important to ensure **proportionality** in the CRA to guarantee fair competition. For instance, allowing **self-assessment at a certain level of nature, scale and complexity of organisation** (i.e. SMEs).
- The EU should promote incentives for manufacturers to produce more secure ICT products ("security by design") and to guarantee a **risk-based cybersecurity approach** from early stages of product development ("security by development").
- The EU should set up an **EU-wide process on the transparency of ICT products'** functionality that would help to communicate to consumers the cybersecurity level of ICT products.
- A **transitional period** in any form of EU intervention should be foreseen for companies to adapt given the quick evolution of cyber risks and threats.

2. General comments regarding cyber resilience

While cyber resilience of digital products and ancillary services is important, it is only a partial element of cyber resilience. It is our assessment that cyber resilience is often viewed through the prism of IT issues alone. This can leave organisations, and the economy more generally, exposed to cyber-risk attacks that might come from other areas (i.e. beyond products or services).

An overall global risk management approach to EU cyber resilience is therefore recommended. This would assist organisations in:

- identifying
- assessing; and,
- treating cyber risks.

For instance, FERMA has recommended a cyber risk governance model that could provide guidance to organisations in this area[1].

[1] FERMA and ECIIA Cyber Risk Governance Report: https://www.ferma.eu/publication/ferma-eciia-cyber-risk-governance-report/

Cyber is increasingly a systemic risk. This has clear implications for the way that EU enterprises will treat their risks. FERMA is therefore pleased to see that the European Commission has placed cyber insurance as part of its reflections on the CRA in the consultation questionnaire.

FERMA provides the following observations on the topic of cyber insurance. While FERMA acknowledges that cyber insurance can help organisations raise their cybersecurity levels as it can effectively audit their cybersecurity, there are some problems, notably that:

- cyber insurance often does not provide EU enterprises with sufficient financial protection covering only a part of the total amount of potential damage; or, coverage may be available but unaffordable; and,
- There is not yet a widespread take-up of cyber insurance. In fact, research from AMRAE (the French risk management association) found that in 2020 only 8% of medium-sized enterprises in France have cyber insurance coverage.[2]

FERMA also believes that captives[3] might be considered as an additional pillar for cyber insurance for enterprises of a certain size, nature and risk profile to respond to the market inefficiency.

FERMA provides the following general recommendations for consideration in the CRA initiative:

- We call on the European Commission to aim to foster **a global risk management approach** to cyber resilience. This could draw on FERMA's work in the area of cyber risk governance[4], for instance.
- The EU has a key role to play in terms of **raising levels of education and awareness** of cybersecurity by making sure there is enough training and resources allocated to it (especially for smaller companies). It is also important to promote cybersecurity programmes for professional users.
- The EU should explore the creation of **a European cyber pooling or compensation fund**, which could both support the private insurance market and step-in when the insurance market cannot fully meet the coverage needs of companies, in the framework of a public-private partnership (PPP) for instance. FERMA has in the past called on the European Commission to create a framework for catastrophic risks through a PPP.[5] Here, inspiration could be drawn from existing pools (e.g. terror).
- It is important to allow **more flexibility for captives** since they represent for enterprises an additional risk management tool. As such, it is important that proportionality in the prudential regulation (Solvency II) is ensured.

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

[2] AMRAE Project LUCY Report: https://www.amrae.fr/recherche?type=All&search_api_fulltext=project+LUCY
[3] A captive is an entity set up and owned by a corporate group to insure or reinsure certain risk
[4] FERMA and ECIIA Cyber Risk Governance Report: https://www.ferma.eu/publication/ferma-eciia-cyber-risk-governance-report/
[5] FERMA Position Paper on 'Building an EU Resilience Framework for Catastrophic Risks https://www.ferma.eu/ferma-calls-for-eu-resilience-framework-for-catastrophic-risks/