POSITION PAPER

Brussels, 29 April 2022

Orgalim position on the future Cyber Resilience Act

Executive summary

The rise of cyberattacks and hackings in the economy, and a society that increasingly relies on digital solutions and new technologies to innovate, create the need for a common European solution that can help build cyber resilience and security. In response, the European Commission intends to put forward its Cyber Resilience Act (CRA) proposal in the third quarter of 2022, aiming to establish common standards for cybersecurity products.

Orgalim welcomes the Commission's initiative and is convinced that a coherent regulatory framework is of the highest importance, especially in the context of the smooth functioning of Europe's Single Market. We believe that in order for the Act to be workable, effective and meaningful, the following elements should be taken into account.

1. The CRA must create legal certainty across all connected products
2. Essential requirements are the basis for the cybersecurity of connected products
3. Conformity assessment must be based on risk and allow for self-assessment for the majority of connected products
4. Harmonised European standards should be the preferred way of describing technical details
5. The CRA should build on the New Legislative Framework (NLF) to clarify responsibilities after a product is placed on the market
6. Effective market surveillance will be key

Introduction

In November 2020, Orgalim called for a horizontal legislation on cybersecurity[1] for networkable products within the existing New Legislative Framework (NLF). In December 2020, the Council highlighted the need for a horizontal legislation and, shortly after, the EU Strategy on Cybersecurity outlined how an "Internet of Secure Things" could be achieved by horizontal rules. Now, the Cyber Resilience Act (CRA) has been announced for the third quarter of 2022, aiming to be the regulatory tool to put these ideas into practice.

[1] In this position paper we use both terms "cyber resilience" as coming from the term "Cyber Resilience Act" and "cybersecurity" as a widely used common term. We refer to "cyber resilience" as a more macroscopic term addressing an objective for the EU. "Cybersecurity" refers to a special type of requirements for products.

Especially in the context of the smooth functioning of Europe's Single Market, we believe that a coherent regulatory framework to cover the cybersecurity of connected products throughout their life cycle, proportional to the risks, is of the utmost importance. Based on proven success factors within the NLF regulation, in this position paper Orgalim reinforces the message set out two years ago, and we list what we consider to be the cornerstones of the upcoming CRA.

1. The CRA must create legal certainty across all connected products

In recent years we have seen a diversity of new product legislation or proposals that include cybersecurity requirements (e.g. the Draft Machinery Products Regulation, delegated acts under the Radio Equipment Directive, the Medical Devices Regulation, the Draft General Products Safety Regulation and others). In this context, we particularly welcome the Commission's words in the recent consultation on the CRA and the associated "Call for Evidence for an Impact Assessment": *"This intervention would aim to improve the Internal Market's functioning by: (i) streamlining and supplementing existing rules; and (ii) preventing further fragmentation of cybersecurity requirements […]".*

In the context of that consultation, the details of products within its scope are worthy of further discussion. Meanwhile, we would like to point out that in order to provide the necessary legal certainty, the scope of the CRA should be wide enough to create coherence across the products currently regulated under the NLF, but specific enough to only address products or product components that can undergo, or be part of, a cyberattack.

We therefore propose to address 'connected products', which are products intended to communicate by themselves over the internet, regardless of whether they communicate directly or via other equipment[2]. For any such connected product the cybersecurity requirements and corresponding conformity assessment must be covered by only one legislation.

The goal of the CRA should therefore be to harmonise the regulatory landscape for the cybersecurity of products under one central, consistent, and coherent reference point. The CRA is the opportunity to create certainty for all stakeholders vis-à-vis existing and upcoming cybersecurity provisions across separate regulations, for instance by explicitly stipulating that conformity with one must provide conformity with the other.

Last but not least, being horizontal in scope, the CRA should avoid overlaps with legal obligations on entities such as in the NIS2 Directive, and it must also clarify the role of cybersecurity schemes possibly emerging from the Cybersecurity Act.

2. Essential requirements are the basis for the cybersecurity of connected products

In order to allow for the above-mentioned horizontal approach, the CRA should set out technology-neutral essential requirements for cybersecurity in the form of requirements common to the connected products that are within its scope, where required by a risk analysis. More specifically, additional requirements of cybersecurity should be addressed in harmonised European standards (see point 4 below).

[2] See "Orgalim comments on the draft delegated act for internet-connected radio equipment and wearables"

3. Conformity assessment must be based on risk and allow for self-assessment for the majority of connected products

The CRA should build on the conformity assessment procedures that are set out in the current NLF (Decision 768/2008), which have to be applied depending on the intended use and the risk assessment for the respective product with a special role for what is referred to as module A ("internal production control" also known as "self-assessment").

Self-assessment provides a sufficient level of security and the experience with, for example, the Electromagnetic Compatibility Directive (EMCD), the Low Voltage Directive (LVD) and the Radio Equipment Directive (RED) serves as a clear and comprehensive proof of this. Third party certification is much more burdensome and less agile, and there is no evidence that third party conformity evaluation is necessary to ensure a satisfactory cybersecurity level.

Moreover, promoting self-assessment is an investment in the future of Europe – which is widely acknowledged to lack cybersecurity skills and trained personnel. It is important to note here that manufacturers know their product better than external parties, and for many of them, the know-how of the software architecture and the measures needed to prevent cyberattacks are the core of their business. The use of self-assessment will lead to a further cybersecurity learning curve (and which should be accompanied by more public authorities' support towards training, development of competencies, etc.) meaning that the manufacturers will provide better cybersecurity and will thus play an important role as the backbone of a cybersecure Europe.

Also, self-assessment is linked to faster time-to-market, which is an important element for the competitiveness of European manufacturers and something that the Commission is keen to support through other initiatives, including the new Standardisation Strategy. Therefore, both SMEs and large businesses need flexibility of choice between assessment procedures.

Lastly, third party certification can – especially in an economy with high innovation cycles – create a bottleneck due to the limited capacity of notified bodies. Given the millions of connected objects, self-assessment should always be an option for conformity assessment in the future CRA.

4. Harmonised European standards should be the preferred way of describing technical details

The core principle of the CRA should be – as in the NLF – that only essential requirements are stipulated in the law in a technology-neutral way to keep the law fit for future innovations. Technical specifications should continue to be defined in harmonised EN standards, consistent with international standards, as the technical basis to ensure compliance. The essential requirements must be specific enough to allow for a risk-based conformity assessment, but they should not be prescriptive to a specific technical solution.

The European Standardisation Organisations have the most sophisticated system to democratically ensure three key requirements for reliable technical specifications: 1) consensus; 2) transparency; and 3) inclusiveness.

Also, the use of standards – for instance to reflect changes in the state-of-the-art – makes the legislation more future-proof. This is extremely relevant for cybersecurity with its inherent challenges of the rapid development of both potential attacks and protection measures.

5. The CRA should build on the NLF to clarify responsibilities after a product is placed on the market

In an ever-changing threat landscape, the security of a product can be challenged during its whole life cycle. On the other hand, the manufacturer cannot possibly consider all future malicious threats. However, manufacturers do acknowledge their responsibility for the manufacturing of sufficiently resilient products.

As regards the responsibilities of manufacturers with respect to the above-mentioned issue of product resilience, the CRA should build on measures or procedures to which manufacturers have to adhere, which are generically speaking processes – as opposed to features of a product. Processes are a well-known key element for providing security. They help to ensure security during manufacturing, to manage vulnerabilities, or to cover the whole life cycle of a product. Regulation can address this issue by requiring manufacturers to implement processes. However, the process should be defined in harmonised EN standards consistent with international standards, and the choice of the most suitable process should lie with the manufacturer.

A specific process is the provision of security updates or similar measures after a product is placed on the market. Such updates can be provided in order to counter known risks after the product has been put into service or use. The CRA should build on the NLF when stipulating obligations for economic operators. The obligation should be transparent about the support period for the time after which a product is placed on the market, and should ensure that there is a process in place to provide support. This obligation could be combined with the essential requirement of the product, which is that it has to be technically prepared to receive such updates.

The resilience of a connected product to cyberattacks after it is placed on the market is the responsibility of various stakeholders (e.g. manufacturers, third party software developers, end-users, etc.) so it could be reasonable to stipulate appropriate cybersecurity obligations for economic operators other than manufacturers.

6. Effective market surveillance will be key

Last but not least, effective market surveillance is the key to ensuring the enforcement of compliant products on the EU market, therefore avoiding unfair competition and ensuring the security of end users.

Member States must invest in the know-how and in the skills of their surveillance authorities in order for them to be competent and to take over their responsibilities. A specific challenge to consider would be to not only control the products, but also the obligations relating to the above-mentioned processes over their life cycle.

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438