JBCE's feedback on the proposal for a Cyber Resilience Act

23rd January 2023

Introduction

Japan Business Council in Europe (JBCE) appreciates the opportunity to provide comments on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

JBCE fully supports the aim of improving the cyber resilience of connected products on the EU market, in order to protect the data of consumers and other societal stakeholders and to improve the resilience against an ever-increasing number of threats from cyberspace. However, we would be happy to provide our recommendations to improve the legislative proposal. Our response focuses on several aspects: the relationship with other legislation, the scope of products affected and the alignment with the New Legislative Framework. We would also like to highlight some potential risks of creating unintended cybersecurity issues. Finally, although we do feel the issue is urgent, we suggest that a longer transition period is provided to allow manufacturers sufficient time to adjust their products and processes to the new requirements.

Horizontal legislation

The proposal for the Cyber Resilience Act ("CRA") clearly intends to cover the issue of harmonization between different legislation containing cybersecurity elements. This will close the gap for unsecure hardware products and makes it clear to economic operators which legislation prevails. It will also set a mandatory level for cybersecurity requirements and establish the processes that need to be followed by economic operators. JBCE appreciates this approach to ensure coherence and consistency but remains concerned about the relation with the Radio Equipment Directive (RED) and delegated regulation 2022/30. As the RED itself was not written with cybersecurity in mind and the delegated regulation does not cover the lifecycle of the product, the delegated regulation can only ensure that a subset of radio equipment is compliant at the specific moment of placing it on the market. Due to these basic deficiencies of the RED delegated regulation, JBCE supports repealing the delegated regulation as suggested in the CRA's introduction and Recital 15.

Scope of the proposal

With respect to the scope of the proposal, we want to offer the following considerations.

Finished products

The scope of the CRA includes any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately. The industry is very familiar with hardware products and their embedded software, but not with the further extension to any standalone software or any components.

In order to ensure the CRA's success, it would benefit from an alignment with other product-specific legislation and restriction of the scope to finished hardware products that manufacturers control and that can be assessed in a holistic way. Requesting that all components comply will considerably change the current way of working as typically product legislation only applies to finished products that are placed on the market (ref. Blue Guide clause 2.1). Assessing components might also be irrelevant as

the intended use of the 'end product' might differ from the intended use of a component. It is also noted that combining multiple compliant components into a finished product does not mean that the end product would be compliant (CE + CE ≠ CE). The finished product is the one that needs to address the final cybersecurity risk.

Software components

Additionally, the complexity of combining finished hardware products with software components will make market surveillance very hard, for example in the case where the user of a smart product installs third-party apps via an Android app store. While the responsibility for the smart hardware product is obvious, the compliance of the software might be less clear. Therefore, JBCE suggests limiting the scope of the CRA to hardware products with their embedded/ancillary software. By keeping a few, specific components listed under ANNEX III, the inclusion of these security-relevant components can still be ensured without affecting the vast majority of other insignificant components and standalone software. By setting a familiar scope of finished products, it is anticipated that the CRA can be implemented efficiently by all stakeholders.

Open-source software

Annex III lists critical products with digital elements, for example, under class II, point 1, "Operating Systems for servers, desktops and mobile devices". Open-source is explicitly excluded from the requirements of the act (recital 10). Examples of this would include, in broad terms, the exclusion of Linux and FreeBSD. However, under the current recital, open-source used in "commercial activities" is not excluded. In this context, the understanding is that support and maintenance services on open-source projects that include any commercial benefit are specifically included. There could be a significant imbalance between open-source ventures compared to commercial software counterparts, with open-source ventures developing very widely implemented software components, but often receiving a fraction of the commercial benefit that commercial software ventures would (when also including the same component). Considering that open-source also drives innovation and rapid advancement in almost all areas of critical products, it is necessary to include additional ringfencing around the specific CRA requirements for open-source products, including those used in "commercial activities" to avoid constraining or burdening essential open-source activities and ultimately stifling open-source innovation and contribution within the European Union.

Devices protected as a system

Special consideration should be given to devices that are protected as a system. For example, Unified Threat Management (UTM) is an information security system that provides a single point of protection against threats, including viruses, worms, spyware and other malware as well as network attacks. While the UTM itself is clearly within the scope of the CRA, each device under UTM's protection on the premise should be excluded.

Critical products with digital elements

Annex III contain the list of critical products with digital elements. In order to better understand which products fall in scope and to avoid a different interpretation by stakeholders, further clarification would be needed in guidance documents prepared by the Commission (e.g. Class II, Point 8 lists "Secure Elements" is a too vague a definition).

The NLF concepts

JBCE very much welcomes that the proposed regulation is based on the well-known New Legislative Framework. Familiar conformity assessment procedures and obligations for economic operators will help the industry to adopt this new legislation smoothly. By setting the cybersecurity requirements for products and processes via Essential Requirements, the legislation will be future proof. Societal stakeholders can take part in an inclusive process of drafting Harmonised Standards, ensuring that those Harmonised Standards will keep pace with technological developments and can be tailored to specific categories of products. Finally, the NLF conformity assessment modules will ensure a risk-based approach, setting stricter requirements for the most critical products.

Nevertheless, we believe a few items could benefit from improvements:

- Standalone software
  It is unclear how the familiar concepts of the NLF can be applied to intangible products, such as standalone software, especially concerning the marking requirements (CE mark, visible sign, e-mail and postal address of manufacturer/importer). This point was already raised in the recent report on the evaluation[1] of the NLF.
  More significantly, the economic operators' roles are also less obvious in our opinion. For instance, if third-party applications can be installed by the user via an app store on a smart product, clarity is needed on the app store's role as an importer or distributor. In general, we would recommend carefully analyzing the risks linked to the adaption of the NLF for software compliances before applying it to a vast number of intangible products.
- Contact information
  The CRA proposal requires an e-mail address for the manufacturer and the importer to be added on the product in addition to the postal address. Under the usual NFL legislation, this postal address is used by market surveillance authorities to identify the responsible person for compliance. Until now, an e-mail address was never required on the product/packaging. In addition, the information and instructions to the user need to contain a point of contact where information about security vulnerabilities of the product can be reported and received. JBCE is worried that 3 different points of contact on the same product will confuse the end user and would suggest removing the requirement for the manufacturer/importer's e-mail address. Having only 1 point of contact in the user instructions should be sufficient for reporting any vulnerabilities.
- Testing requirements for Notified Bodies
  The conformity assessment for Module B (EU-Type Examination) as described in Annex VI requires that the EU-type Examination be carried out by assessing the adequacy of the technical design, plus examining specimens of one or more critical parts of the product. The 'examination of specimens' is typically not required under NLF legislation such as the Radio Equipment Directive and requires a Notified Body to carry out appropriate examinations and tests. Notified Bodies typically perform a review of the technical documentation and processes while the testing itself is performed by the manufacturer or a third-party test laboratory. Hence, introducing additional testing by the Notified Bodies is expected to result

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12654-Industrial-products-evaluation-of-the-new-legislative-framework_en

in extra work and lead times, while cybersecurity experts are already a scarce resource and while this offers no real additional benefits.

- Recognition of international standards by Notified Bodies
  In the case of critical products with class II digital elements, the involvement of a Notified Body will be required. To ensure international alignment and avoid fragmentation and overlap, it is recommended that the use of internationally recognized standards is accepted in these conformity assessment procedures involving Notified Bodies, such as:
  - ISO/IEC 27001 (information security management)
  - IEC 62443-4 series (Security for industrial automation and control systems), IEC 62443-4-1 focuses on the Secure Development Lifecycle (SDL)
  - IEC 62443-3-2 (Security risk assessment for system design)
  - IEC 29147 (vulnerability disclosure)
  - Etc.
- Available cybersecurity certification schemes and international standards
  As it stands, it is very complex to navigate the available international standards and certification schemes that could be used for demonstrating compliance.
  Article 18(4) recognizes the use of cybersecurity certification schemes. JBCE recommends that the Commission adopts such implementing acts as soon as possible, to achieve legal certainty about the methods available to demonstrate compliance under the CRA.
  Furthermore, in as much as there is existing recognition for certain international standards (mentioned in the previous item) as per the Cybersecurity Act[2], these should be explicitly listed in a separate Annex or guidance document.
- EU Declaration of Conformity
  Article 10(11) contains the requirement to either bundle the EU Declaration of Conformity with the product or publish it on the website and include the internet address in the instruction manual. While a similar requirement already exists for products within the scope of the Radio Equipment Directive, the majority of products falling in scope of other product legislation (EMC Directive, Low Voltage Directive, Machinery Directive) do not have such an obligation. In order to align with this other legislation, the EU Declaration of Conformity should be kept at the disposal of the market surveillance authorities and provided on request only. In addition, for products (e.g. components, software) not falling under any other product legislation, including the EU DoC in the operating manual should be permitted. Requesting that the DoC be provided with each component or software would cause a heavy burden on logistics and have an impact on the environment.
- Cybersecurity risk assessment
  Article 10(3) indicates the need for a cyber security risk assessment. However, a concrete/generic example of an assessment procedure and/or documentation is not provided. JBCE would welcome if a template for cybersecurity risk assessment or reference to an existing standard on risk assessment were provided in an Annex or guidance document.

[2] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Reporting obligations

With respect to the reporting obligations for actively exploited vulnerabilities and incidents, JBCE would like to highlight a few suggestions for better alignment and operational efficiency:

- Alignment with NIS2
  The requirement of Article 11 to report within 24 hours, implies that manufacturers could require the availability of engineers and cyber security specialists on a full-time basis (24/7). However, only a few large enterprises can establish such organizational structures for this reporting requirement. It is difficult for SMEs, including startups, to comply with these requirements. This would be highly detrimental to the interests of the market.
  Instead, we recommend introducing the 3-step approach contained in the NIS2 directive[3]:
    - Early warning within 24 hours.
    - Incident notification within 72 hours.
    - Final report no later than one month after notification.

  It is worth noting that it is not always easy for a manufacturer to determine whether the incident is caused by unlawful or malicious acts or has cross-border impact. Also, as NIS2 requires only reporting for 'significant incidents', alignment in this respect is welcomed. In any case, further guidance on criteria to determine severity and impact is needed.

- Exploits of vulnerability reports
  Attacks by malicious entities include false incident reports. The attack impedes the activities of both ENISA and manufacturers. The recommended time to start reporting to ENISA is therefore once the incident has been correctly identified or evaluated and reproduced by the manufacturer. Manufacturers also need sufficient time to defend themselves against those false incident reports. Otherwise, manufacturers will continue to risk unnecessary CRA penalties from malicious attacks.
  JBCE recommends that it is clearly stated that the trigger of the manufacturer's reporting obligation is only when manufacturer has verified a vulnerability, which also means that the manufacturer investigates reports from other entities and recognizes that a real vulnerability exists, not when other entities report to ENISA and/or the manufacturer. Of course, manufacturers shall be obliged to manage and verify vulnerability information brought to them by other entities.
- Reporting requirement to the person/entity maintaining a component
  Article 11(7) indicates that manufacturers shall report a vulnerability to the person/entity maintaining a component. The question arises of how notification would be handled in the event of a component no-longer maintained, maintained by several independent groups, and/or an open-source component without a clearly identified maintainer (for example, multiple source code repositories).
- Reporting template

[3] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Article 11(5) indicates that the Commission may further specify the type of information, format and procedure of the reporting. As the same requirement exists under the NIS2 Directive, again alignment with that format is requested. However, it would also be beneficial to include a generic template of the report format in a separate Annex or guidance document.

Concerns on cybersecurity

The aim of the CRA is to strengthen cyber resilience in the EU. In this regard, we believe care should be taken that the proposal does not introduce unintended security loopholes by setting transparency obligations. Indeed, such publicly available information could provide easy sources for malicious entities about which products to target for:

- Reporting to ENISA
  Manufacturers must report actively exploited vulnerabilities and incidents having an impact on the product's security to ENISA. As the single agency receiving those reports from all manufacturers placing products on the EU market, ENISA might become targeted by malicious entities, potentially leading to high cybersecurity concerns.
- Software Bill of Materials (SBOM)
  If the vulnerabilities need to be included in the Software Bill of Materials (Annex I, 2(1)) and the information where the SBOM can be accessed is made available to end users (ANNEX II (6)), this could provide easy information to malicious entities.
- Ceasing manufacturers
  If a manufacturer ceases operations, the economic operators (manufacturer, importers and distributors) need to inform the relevant market surveillance authorities and users of this. Again, this could provide easily accessible information on vulnerable products.

Timeline

While JBCE fully understands the sense of urgency of the proposal, manufacturers need to be provided with sufficient transition time to meet the new obligations. The RED delegated regulation showcases the fact that a 24-month transition time is not sufficient[4]. Indeed, additional time is needed to adopt Harmonised Standards, to implement the changes in product design and for Japanese manufacturers to ship compliant products to the EU market.

By introducing components in scope, an extra delay is introduced. Equipment manufacturers incorporating components can carry out conformity assessment and prepare technical documentation, etc. only after the completion of the conformity of the components. Therefore, it is necessary to separate the deadlines for components and equipment. JBCE therefore recommends a transition period of 4 years for components and 6 years for finished products.

In addition, JBCE members are concerned about the requirement for products already on the market that are subject to substantial modifications of Article 55(2). For example, a general-purpose

[4] CEN-CENELEC letter of 13 December 2022 to DG GROW 'Request for amendment of M/585 – Standardization Request as regards Radio equipment in support of Directive 2014/53/EU' requesting to postpone the deadline for the adoption of the cybersecurity related Harmonised Standards by 9 months and to consider a postponement of the date of applicability of the Commission delegated regulation (EU) 2022/30 in alignment with the Standardization Request.

controller such as a Programmable Logic Controller (PLC) can be used for various purposes depending on the final system developer. Some of those PLCs were placed on the market 15-20 years ago, but are still in use. If new software loaded on such a PLC is regarded as “substantial modifications in intended purpose” the manufacturer would be required to support those legacy devices for an unreasonably long time. For reasons of simplification, it is recommended that the CRA only apply to products placed on the market after the date of applicability.

About JBCE

Founded in 1999, the Japan Business Council in Europe (JBCE) is a leading European organisation representing the interests of over 95 multinational companies of Japanese parentage active in Europe. Our members operate across a wide range of sectors, including information and communication technology, electronics, chemicals, automotive, machinery, wholesale trade, precision instruments, pharmaceutical, textiles and glass products.

For more information: https://www.jbce.org/ / E-mail: info@jbce.org
EU Transparency Register: 68368571120-55