AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Cyber Resilience Act proposal

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.4 trillion in 2021, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

As the European Commission aims to strengthen the EU's cybersecurity policy through the Cyber Resilience Act (CRA), it must ensure that all industry concerns are taken into consideration, as these will be key for the successful adoption and implementation of the CRA. In particular, the current proposal should be adjusted to further clarify and develop aspects such as scope, conformity assessment procedures and reporting obligations.

Introduction

As the EU economy becomes more digitalised, the challenges related to cybersecurity continue to increase and evolve, in particular cyber-attacks. Products with digital elements represent a key vector used to conduct malicious cyber-attacks. In order to enhance market confidence, it is fundamental to ensure the security of the entire supply chain by enhancing the safety of products in the early stages of their technical design and development.

The proposed CRA is an important opportunity to enhance the security of products with digital elements. The Commission's decision to **introduce a set of horizontal and risk-based rules**, which allows conformity to be demonstrated with **self-assessment as a default method,** is highly appropriate for such goal. In other to further enhance the proposal, the following paper outlines several recommendations to **improve and further clarify aspects of the proposed regulation**.

1. Scope

While the European Commission has taken a notably transparent and inclusive approach in preparing this substantive piece of legislation – in particular through an extensive stakeholder consultation – the scope of the CRA, as proposed by the European Commission in September 2022, remains overly broad. For example, the CRA would potentially apply to the entire life cycle of any tangible product containing connected digital elements. It would also require that covered products be delivered without any known exploited vulnerabilities and reporting not only of cyber incidents, but also for actively exploited vulnerabilities.

The Commission has also rightly referred to existing legislation (eg Medical Devices Regulation 2017/745[1], In Vitro Diagnostic Regulation 2017/746[2], Motor vehicle Regulation 2019/2144[3] or Aviation Safety Regulation 2018/1139[4]), which demonstrates its effort to avoid regulatory overlap of requirements and enforcement, as well as unintended double reporting obligations (The Network and Information Security Directive (NIS2 Directive), European Electronic Communications Code (EECC[5]),

[1] Regulation (EU) 2017/745 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

[2] Regulation (EU) 2017/746 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU https://eur-lex.europa.eu/eli/reg/2017/746/oj

[3] Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:02019R2144-20220905

[4] Regulation (EU) 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139

[5] Directive establishing the European Electronic Communications Code (Recast) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972

General Data Protection Regulation (GDPR[6])). However, overlaps in reporting obligations and layers of supervision remain between CRA and the NIS2 Directive[7], as at least some cloud services providers are likely to be subject to both legislations. The proposed exclusion of Software-as-a-Service (SaaS) except for 'remote data processing solutions' in Recital 9 is not clear enough, and it conflicts with the definitions in article 3(1) including 'any software'. Yet, cloud services (including SaaS) will need to comply with all the NIS2 cybersecurity and risk management requirements, making compliance with the CRA requirements unnecessary and likely counterproductive. These overlaps might deter businesses from using cloud-based software at a time when the EU wants three out of four companies to use cloud computing services by 2030.[8] Private-public discussions must take place to ensure legal certainty and proportionality for cloud service providers.

The proposed CRA and the Data Act[9] may overlap, *inter alia*, with 'manufacturers of products and suppliers of related services placed on the market in the Union'. Moreover, in order to avoid conflict and allow for interoperability (eg standardisation), the interplay between cybersecurity requirements in other proposed EU legislation covering different sectors (ie the Digital Operational Resilience Act [DORA][10], Network Code for Cybersecurity of Cross-border Electricity Flows[11]) and the harmonisation of CRA requirements with foreign legislation (ie US legislation) should be avoided conflict.

In relation to DORA, financial entities do produce products with digital elements. However, these are governed under their internal information and communications technology (ICT) risk management framework, as are all financial services that they provide. Therefore, requirements in the proposed CRA, such as incident reporting and vulnerability management, would directly duplicate what financial entities are already required to put in place by DORA. There has been some confusion in the industry with the suggestion that DORA is not a *lex specialis* in regard to products with digital elements, as this implies that such products (eg retail banking application) are not currently subject to oversight and supervision by financial regulators under DORA.

Therefore **it is essential that the legislators clarify the interaction between the CRA and these instruments** to avoid duplicated or inconsistent requirements on economic operators.

Global software and hardware entities generally have a good notion of cyber risks and how to manage them. The scope needs to be approached from a **risk-based** perspective by a clearly defined methodology for determining the limitative list in ANNEX 3. Unfortunately, this not the case, as entities responsible for products in scope of CRA have no clear understanding of how and when their products will be in scope, nor under which categorisation.

The Commission's proposal (article 6[2]) to adopt delegated acts to amend ANNEX 3 reflects the clear intention to make future-proof legislation. However, the exact process and methodology should be

[6] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[8] Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030, European Commission Press Release, 9 March 2021 https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

[9] Proposal for a Regulation on harmonised rules on fair access to and use of data https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN

[10] Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

[11] Network Code on sector-specific rules for cybersecurity aspects of crossborder electricity flows (NCCS), https://www.acer.europa.eu/sites/default/files/documents/Recommendations/Revised%20Network%20Code%20on%20Cybersecurity%20%28NCCS%29_1.pdf

more transparent and economic operators should be structurally involved. An **open and transparent framework** that consults industry stakeholders on modifications of the scope or ANNEX 3, is needed.

Similarly, the definition of **open-source software** needs to be elucidated. While it is clear that they are not covered by the Regulation, the circumstance in which software are considered 'developed or supplied outside the course of a commercial activity' is overly vague and deserves clarification.

2. Obligations for economic operators

The ways in which the conformity assessment procedure must be carried out depend on the classification of a product as 'critical', given that not all products pose the same level of cybersecurity threats to the economy. While this creates considerably **different compliance costs** for companies depending on the category of the product, the proposal does not clearly explain how these different costs relate to the risk linked to the different categories of product. To incentivise compliance, it is essential for regulators **to illustrate the rationale of the differing obligations**.

For example, the requirement in Annex I- 1(2) to deliver a product **'without any known exploitable vulnerability'** is not a realistic bar to set: security is always going to be a moving target, influenced by the product's deployment environment, the development of different technologies and evolving cyber-attacks. Such a requirement would discourage manufacturers from conducting meaningful security testing, leading some of them to avoid scanning products (this way, keeping those potential vulnerabilities 'unknown'), and thereby introducing less secure products to the market. Instead, a **risk-based approach to remediating vulnerabilities**, based on numerous factors and situational circumstances like the vulnerability risk level and the criticality of the data and the systems impacted. Such an approach would allow entities to focus on remediating the most critical vulnerabilities first and would also be aligned with existing global industry standards and frameworks.

Additionally, manufacturers shall ensure the conformity of a product with digital elements for the expected product lifetime or for a **period of five years** – whichever is longer. Imposing this obligation on manufacturers for such a long timeframe will likely hinder innovation, disincentivise SMEs and decrease EU global competitiveness. To avoid this **the proposal should be aligned with the EU consumer protection framework**, whereby sellers are liable to the consumer for any lack of conformity for a period of two years.

Further clarity is also needed in relation to products that are **already placed on the market** before the date of application of the Regulation, which have to implement conformity requirements only if they are subject to 'substantial modifications' in their design or intended purpose. Thus, legislators should clearly define the notion of **'substantial modification'**, in order to provide legal certainty to manufacturers seeking to comply with the CRA. The current language is too broad and may suggest that operators would need to undergo a conformity assessment procedure every time the software is updated, which happens too frequently for organisations to credibly keep up with the assessment and documentation process. Therefore, it should be clarified that the conformity assessment procedure only needs to be undertaken **upon a major version upgrade only.**

Similarly, Art 19 provides extensive powers to the Commission in drafting common specifications. Therefore, that proper time needs to be given to European and even international standards development organisations (SDOs) to develop security standards before common specifications are even considered. It must be clear what the considerations are to make use of this article, it should be an emergency provision (last resort). Moreover, Art 19 needs to include proper mechanism for

transparent and comprehensive engagement with industry. This will ensure better monitoring of the market more evidence-based policymaking.

Finally, some ANNEX 5 requirements would oblige manufacturers to share sensitive information externally. Publicly disclosing too many details about the product in the technical documentation (such as complete information about the product's design, development including system architecture or software components) as well as detailed risk assessments, could significantly increase confidentiality, intellectual property and security risks, thereby increasing the likelihood that malicious actors actively exploit such information. Better safeguards should be included in the text so that necessary information sharing between manufacturers and government authorities is not more exposed to malicious attacks.

3. Incident reporting

Legislators should further clarify the procedure for incident reporting outlined in article 11. It is essential for national competent authorities of each Member State to have a detailed and comprehensive description of each phase of the process and **consider the differentiation between reporting exploited vulnerabilities and incidents** regarding the products that are already on the market.

The term 'actively exploited vulnerability' should be clarified as to whether this is about an incident on the product itself, or an exploitation that could potentially impact the product. The latter would be classified as a Product Security Incident Response Team (PSIRT) issue, which typically is not reported externally or to a competent authority until a fix/patch has been made available, in line with existing vulnerability handling best practices and standards to protect customers. Releasing public information about an unmitigated vulnerability can lead to additional cyber-attacks and is out of step with global industry best practices.

Moreover, the Regulation should align with existing or draft legislation covering cyber incidents (such as NIS2, DORA, CER Directive[12], EECC, NCCS, GDPR), in order to avoid the application of conflicting and disproportionate notification obligations on operators. While under the CRA all cyber incidents must be notified, under the NIS2 Directive only incidents 'having a significant impact on the provision of [Member States'] services' are subject to a notification obligation. In addition, under the CRA, incidents must be notified to European Union Agency for Network and Information Security (ENISA). On the other hand, under the NIS2 Directive the central role in the notification procedure is played by the relevant national competent authorities or by one of the Member States' computer security incident response teams (CSIRTs). **The incidents that must be notified and the relevant competent authorities must be aligned, as these inconsistencies can significantly impact the overall product security by creating unnecessary uncertainty for the manufacturers that need to undertake such reporting processes.**

Finally, ENISA plays a central role in the incident reporting procedure, as it is responsible for receiving and forwarding all notifications. However, the agency's limited capacity causes significant concerns. Therefore, the deadline for reporting should be extended to 72 hours so that the economic operators are able to provide the maximum of actionable information and intelligence. ENISA should also adhere to a clear deadline to notify the member state authorities. This should not be with undue delay in their role as intermediary and facilitator (information broker)to the CSIRTS and member state authorities.

[12] Proposal for a Directive on the resilience of critical entities https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

Additionally, it must be ensured that there are structural public-private cooperation mechanisms to discuss the analysis, mitigation and subsequential follow-up to this reporting.

4. Transition period

It is crucial to establish realistic **transition period** for the implementation of the CRA. Since this is a horizontal regulation, the scope includes not only digital products but also a wide range of agricultural tractors, agricultural machinery and construction machinery, many of which are small in volume and/or designed for specialised operations. The applicability of CRA would require design-changes to hardware and software architecture of all these machinery products. Additionally, machinery products already have to deal with the Cybersecurity requirements brought in place by the revision of EU Machinery Products Regulation[13], with an implementation timings of 2026. Therefore, it would be fair to propose **at least 72 months** for the implementation period for CRA. A staggered approach to implement a subset of CRA to the machinery products first and then the full set of CRA requirements, a few years later, could also be looked upon after further evaluation and discussion.

Moreover, a clear timeline needs to be introduced for compliance with any changes in the CRA – such as scope and requirements – which the Commission is empowered to introduce through implementing and delegated acts. Economic operators must have a clear guidance and proper time buffer to conform with the new rules.

Conclusion

The current CRA proposal contains numerous nuances, including the uncertainty on how the CRA will interact with other legislative instruments, the excessive breadth of the scope and the lack of specific guidelines on the applicability of certain regulations or definition of used concepts such as open-source software. Additionally, cost-related issues within the Conformity Assessment Procedure, and procedure unclarity during incident reporting, should also be reconsidered.

In order to strengthen cybersecurity policy within the Union, European institutions must continue to have an open-dialogues with the key stakeholders, including industry, and consider their key concerns.

[13] Proposal for a Regulation on machinery products https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0202