POSITION PAPER

Cyber Resilience Act: Proposal for a Regulation on cybersecurity requirements for products with digital elements

May 2023

Key points

- SBS **welcomes** the proposal for a Cyber Resilience Act (CRA) by the European Commission, as it is a necessary step to **strengthen the security of connected devices and services in the European Single Market**, fostering cybersecurity all across the supply chain. However, it stresses the issue of the additional costs generated by new mandatory requirements for SMEs, including start-ups, who play a key role in this sector. If the possibility for voluntary cybersecurity certification cannot be deemed an option for SMEs, it calls for a degree of **proportionality as well as increased guidance and resources** for SME implementation of the new requirements, to lower compliance costs.

- When **identifying suitable standards** to be used in conjunction with the CRA requirements, the impact upon smaller companies should be considered. Measures should be taken to guarantee effective SME representation in cybersecurity-related standardisation committees.

- The co-legislators should also consider the establishment of **regulatory sandboxes**, based on the model that is introduced in the Artificial Intelligence Act. Public authorities at the national level should notably provide the right conditions to make regulatory sandboxes effective for SMEs, which tend to struggle in creating suitable testing environments.

- While SBS endorses the proposal's risk-based approach, there is a need for **additional clarity on risk assessment requirements**. Additional clarity regarding the obligations along the **supply chain** – where SMEs often lack a full overview - are also welcome.

Small Business Standards • Rue Jacques de Lalaing 4 • 1040 Brussels, Belgium
info@sbs-sme.eu • sbs-sme.eu • T +32 (0)285 07 27 • Transp. Register 653009713663-08

- The CRA must finally include considerations of **sustainability,** limiting the ability of Original Equipment Manufacturers (OEMs) to impose complex security standards to restrict access to their devices. Moreover, to avoid planned obsolescence, it is proposed that **manufacturers of critical products provide security updates for the entire life cycle of their products, or for a period of five years, whichever is longer.**

Background

A 2021 ENISA report on Cybersecurity for SMEs found that 80% of SMEs claim that a cybersecurity issue would have a serious impact on their business – with **57% of them stating that they may risk having to shut down their business altogether.**

The costs of cybersecurity attacks for SMEs can be large, and often go beyond their available cash reserves. Resilience and adaptability are key to the survival and growth of any business, regardless of their size. Yet, **considering SMEs account for over 99% of all businesses** across Europe, promoting their security is critical to ensuring the security of the European Union.

It is in such a context that on 15 September 2022 the European Commission published its proposal for the Cyber Resilience Act (CRA hereafter), aiming to introduce cybersecurity requirements for products with digital elements. The regulation applies a **security-by-design approach,** whereby manufacturers are obliged to ensure the security of their products throughout their life cycle (from planning to maintenance), by making updates available for at least five years, and by reporting exploited vulnerabilities to the European Union Agency for Cybersecurity (ENISA).

The regulation also offers a distinction between different types of products, based on their risk profile: according to the proposal, 90% of products will require a self-assessment. Critical products (such as password management software, firewalls etc.) will be defined as **Class I** and will **require** the application of a **harmonised standard** or a **third-party assessment**. **Highly Critical Products** (such as operating systems and industrial firewalls) **will be** deemed **Class II** and will necessarily **go through a third-party assessment**.

A prior impact assessment conducted by the European Commission found that the introduction of horizontal requirements of cybersecurity would have **significant benefits** for both consumers and businesses, preventing the formulation of divergent security rules in different countries. Furthermore, the CRA is estimated to reduce the cost incurred in the aftermath of cyber security incidents by roughly 180 to 290€ billion annually – with SMEs to be one of the main beneficiaries of these savings.

In a position paper published in May 2022, SBS member SMEunited had reacted to the European Commission's initiative. While it **generally welcomed** the upcoming piece of legislation, it expressively called for:

- The need for **harmonised and transparent rules**, since SMEs tend to struggle to identify secure solutions and providers;

- The **cost of liability to be borne by manufacturers** and developers, and ensure that retailers – who usually lack product-specific and IT expertise - are not burdened with additional obligations;
- Further **clarifications on the requirement to provide life cycle support for products**.

In December 2022, WKO (the Austrian Federal Economic Chamber - also an SBS member), tabled its own position paper on the CRA. It called for the **possibility of voluntary cybersecurity certification**, expressing scepticism over binding horizontal cybersecurity requirements. It also requested further clarification on the term of "life cycle", as well as making sure – in line with SMEunited's own stance - that distributors are not compelled to 'proactively' search and ensure that products they receive are in conformity with the CRA requirements.

All in all, the CRA proposal - among other key pieces of European legislation on cybersecurity (such as the **NIS2 Directive**, **The Cyber Security Act**, and the **Digital Operational Resilience Act**) - goes in the direction of creating a more secure digital sphere for all products and services in the European Single Market. Nonetheless, **SBS calls for policymakers to bear in mind the additional costs generated by new binding horizontal requirements, especially for SMEs**. If there is no room for negotiation on a possible voluntary cybersecurity certification scheme for SMEs, it highlights the need for proportionality and sufficient guidance in order for SMEs to effectively implement provisions under the Cyber Resilience Act.

Making the Cyber Resilience Act suitable to all SMEs

Harmonisation of CRA Requirements Across European Markets – Addressing Compliance Costs for SMEs

Based on the existing European cybersecurity legislative framework, **SBS supports the harmonisation of requirements** for cybersecurity across multiple domains and hence welcomes the Cyber Resilience Act. However, it stresses the issue of the additional costs generated by new mandatory requirements for SMEs, including start-ups, who play a key role in this sector. If the possibility for voluntary cybersecurity certification cannot be deemed an option for SMEs, it calls for an adequate degree of proportionality to facilitate compliance.

Moreover, as with any horizontal regulation, SBS is concerned about the impact of the CRA on products and markets that are already subject to cybersecurity legislation. These markets represent a significant portion of the European Single Market: as such SBS recommends that **sufficient guidance** is made available to SMEs, so that companies can understand the interplay between the different European regulations relating to cybersecurity (Cybersecurity Act, NIS2 Directive, Radio Equipment Directive, Digital Operational Resilience Act…).

Enabling companies to understand those laws without the help of external experts will **lower the cost of compliance**. This is especially true for SMEs who often outsource analysis of applicable legislation. SBS therefore encourages the European Commission and Member States to provide resources, such as financial incentives to help SMEs adapt to the new regulatory landscape. This support can, for example,

be delivered through dedicated information hubs, online training materials, and workshops. Inclusive stakeholder consultations, whereby SMEs would be associated to the different stages of the legislative process until the CRA's full implementation, would further help in that process.

Market Surveillance and Fines

The CRA calls for market surveillance by authorised bodies to ensure that declarations of conformity are valid. SBS believes that designating National Certification Authorities – whose requirements should be harmonised across EU member states at European level, and monitored on a regular basis such as in other sectors like the lifts and machinery industries - to perform market surveillance would simplify bureaucratic processes for companies. Endowing them with sufficient resources, guidance materials and outreach plans will increase legal certainty and decrease compliance friction.

Furthermore, when it comes to the application of fines, those foreseen by Article 53 of the proposal and expressed in terms of amounts or percentage to a worldwide turnover of enterprises are far greater than the resources available to most SMEs. If such fines were to be imposed on SMEs, they would jeopardize their sustainability. SBS would hence suggest that the proposal is adapted such that fines are **levied proportionately.**

Identification of Standards

When identifying suitable standards or certificates to be used in conjunction with the CRA requirements, the impact upon smaller companies needs to be considered. Standards should be achievable for all companies, such that the impact on the market remains minimal. Therefore, **SMEs should be considered as key stakeholders** and actively included in the decision-making process. Too often, large players are the ones who are better able to absorb the costs associated with standards and certifications. Self-assessment and proportionality of conformity assessment should be made possible for SMEs through the development of standards adapted to SMEs. To achieve so, the European Commission should notably install safeguards which guarantee an **effective representation of SMEs in cybersecurity-related standardisation committees.**

In that regard, SBS welcomes the new provision in the European Parliament's ITRE committee's draft report on the CRA, calling for the creation of an **Expert group on Cyber Resilience** with an explicit emphasis on the adequate representation of SMEs. This group could contribute to better identification of relevant standards, suitable for companies of all sizes.

Moreover, such an Expert group could play a pivotal role in **ensuring that the pace of regulation and technological developments are aligned** – a crucial step for up-to-date standards. For instance, new standards of lightweight cryptography algorithms – recently selected in the framework of a program run by the US' National Institute of Technology and Standards – could be essential towards the cybersecurity of Internet of Things (IoT) components and other small devices.

Finally, in the current state of the proposal, critical products classified as Class I will either need to prove their compliance to harmonised standards or undergo a third-party assessment. For the sake of proportionality, SBS suggests that the certificates and standards that are identified as being suitable for Class I products should be:

a. proportional to the security and vulnerability management requirements;

b. in line with the certificates/standards used in other cybersecurity legislation requiring similar security levels;

c. proportional to the profile of the market.

Mandatory regulatory sandboxes at Member State level to support SMEs

To encourage innovation, the co-legislators must take into consideration the introduction of regulatory sandboxes. Based on the measures introduced in the Artificial Intelligence Act, **SMEs can benefit from a sandbox environment that allows them to test their software and cybersecurity products before entering the market.** Regulatory sandboxes can facilitate compliance, boost innovation and contribute to regulatory learning. For instance, SMEs could utilize regulatory sandboxes to understand in which Class their product falls under, and what requirements they must comply with.

In this regard, it is essential that sandboxes become mandatory for Member States to set up, to avoid a fragmented approach in the Single Market. The creation of such real-life test environments is often left to businesses, and while large companies have the financial resources and capacity to build their own test environments, SMEs not always do. Consequently, **it is essential that public authorities at the national level enable the creation of test environments for SMEs**, in order for such regulatory sandboxes to be effective and for SMEs to test the cyber resilience of their products. It is by enabling SMEs to test their products with digital elements in such test environments that public authorities can foster SME compliance to the rules, and therefore level-up European cyber resilience.

Risk Based Approach

SBS strongly believes that the risk-based approach undertaken in the CRA proposal is the right one for identifying which products and software require higher security. Nonetheless, it calls for **greater clarity on risk assessment requirements**. Currently, the regulation mandates every manufacturer to implement specific security measures in its software, without considering the necessity for the specific product and use case. SBS endorses an approach where operators who identify a vulnerability in their risk assessments should adopt measures to mitigate risks to end users. Self-assessment and proportionality of conformity assessment procedures should be facilitated for SMEs through the development of standards tailored to their needs.

Small Business Standards • Rue Jacques de Lalaing 4 • 1040 Brussels, Belgium
info@sbs-sme.eu • sbs-sme.eu • T +32 (0)285 07 27 • Transp. Register 653009713663-08

Moreover, the proposal lacks clear definitions of the risk assessment methods to be used or whether common ones (ISO, NIST, OCTAVE, COSO, AS/NZS, etc.) will be considered equivalent. SBS therefore recommends that the European Commission and ENISA provide a list of recognized risk assessment methodologies and frameworks for SMEs to use as a reference.

The frequency of undertaking risk assessments should also be clarified in the CRA, along with explicit information on the scope, timing, and triggers for reassessment. This would help reduce discrepancies between the burdens imposed on manufacturers by different Member States and prevent any competitive disadvantages arising from divergent requirements.

Lastly, the CRA should clarify whether risk assessments should focus on the application or the implementation of a product, as well as any changes in the product's risk category based on its deployment and use. The environment where a product is deployed and its subsequent use may move a product from one category to another, and the relevant level of compliance should be clarified. To address potential discrepancies in obligations across Member States, **SBS proposes a centralized system for harmonized methods and timing for risk assessments and related processes**, managed by the European Commission or ENISA with input from industry stakeholders.

Supply Chain Obligations

While the New Legislative Framework (NLF) was intended to cover physical products, the CRA covers both hardware and software products. SBS raises the concern that the approach pursued by the scope of the CRA **should fit with the one pursued via the NLF** in terms of improving the internal market for goods, strengthening market surveillance and boosting the quality of conformity assessments. Thus, there is a need to modernise the regulatory approach and differentiate between the requirements for software and hardware.

Furthermore, when laying down obligations along the supply chains, regulators should take into account that **SMEs are often not in the position to have a full overview** and understanding of the different components of a product with digital elements, which are manufactured at different points along the supply chain. This might imply that if obligations are not clearly outlined and adequate support and guidance is not provided to SMEs, they might inadvertently expose themselves to high risks and bear a disproportionate legal and financial burden vis-à-vis large suppliers in their value chain.

More particularly, distributors – which are often SMEs – should not be required to carry out proactive and time-consuming research into the conformity of products. SBS believes they should only act on the basis of the information in their possession, which has been given to them by the manufacturer. In that sense, SBS supports the amendment brought by ITRE's draft report on the proposal (Article 14(3)). Likewise, distributors who build software into their product should only be liable under the scope of being considered as custom manufacturer if they have factual possibilities of influencing the software.

Businesses of all sizes should integrate considerations of sustainability in their operations and produce digital products that last longer. Consumer associations have been denouncing for decades that providers of operating systems or essential hardware often refuse to provide the necessary updates, rendering electronic devices no longer secure or even obsolete. Here is where the Right to Repair and Right to Update become relevant in the context of the CRA, as ensuring the highest cybersecurity standards requires allowing after sales support and maintenance providers "write-mode" access to the data and device.

Hence, it is of prime importance to **limit Original Equipment Manufacturers (OEMs)'s ability to impose complex security standards to restrict access to their devices**. Only then will the after sales market remain competitive and open to the majority of European ICT companies - i.e. SMEs. Therefore, to avoid planned obsolescence and ensure the 'right to repair' for users, **it is proposed that manufacturers of critical products provide security updates for the entire life cycle of their products, or for a period of five years, whichever is longer**. In this regard, SBS welcomes the provision in the European Parliament's IMCO committee's draft opinion on the CRA to align on this requirement. Similarly, the EU Council's decision to remove the five-year limit to the product life cycle in its latest compromise text – meaning that manufacturers are responsible of their product throughout their lifetime - can be backed.

Furthermore, the **requirement to provide life cycle support for products requires clarification**. If a company discontinues a product, it is unclear whether it is still required to provide support and security updates if the product is still in use or accessible. For example, it is still not completely clear whether the company should provide security patches if an app has been discontinued, or been substituted by a newer version. Likewise, the expectations on companies that enter bankruptcy, and their support obligations, should be clarified.

Conclusion

Overall, **SBS welcomes the Cyber Resilience Act proposal's purpose**: on the one hand, increasing the cybersecurity level of connected products and the obligations of manufacturers; on the other, raising awareness on best practices, and encouraging users to report any cyber security threat on their products.

SBS stresses however the **importance that SMEs are included at all stages** of development and implementation of the CRA, to make sure that the needs of the majority of European ICT companies are accounted for throughout all the requirements. This goes, *inter alia*, through the identification of standards adapted to SMEs – but not only, as conveyed along this position paper. By working together, SMEs, industry stakeholders, and regulatory authorities can build a more resilient, secure, and innovative digital ecosystem that benefits all parties involved.

Small Business Standards (SBS) is the European association representing and supporting small and medium-sized companies (SMEs) in the standardisation process, both at European and international levels.

Co-financed by the European Union and EFTA

Small Business Standards • Rue Jacques de Lalaing 4 • 1040 Brussels, Belgium
info@sbs-sme.eu • sbs-sme.eu • T +32 (0)285 07 27 • Transp. Register 653009713663-08