BUSINESSEUROPE

POSITION PAPER

15/03/2023

The proposal for a Cyber Resilience Act

KEY MESSAGES

1. BusinessEurope welcomes the European Commission's proposal for a Cyber Resilience Act (CRA) as it entails the potential to significantly increase Europe's cyber-resilience. We urge the European co-legislators to preserve the CRA's many positive elements, e.g., a self-assessment of conformity for most products. The New Legislative Framework is best equipped to adequately ensure that requirements and obligations for the economic operators are proportionate and aligned with the market practices.

2. The implementation of risk-adequate cybersecurity measures across all products with digital elements during the design, development, and production phases, as well as the vulnerability handling procedures will contribute to a more trusted business environment for the supply and the demand of such products in the EU single market.

3. Targeted clarification on notions such as software-as-a-product and "remote data processing services" must be made to avoid the risk of double regulation, and to ensure that the proposal meets its objective.

4. The risk categorisation of products and thereby the conformity assessment procedures must be clarified based on, *inter alia,* intended use, application environment, method for controlling the product. Highly critical products must be defined in a *lex specialis*.

5. Leveraging harmonised European standards and alignment with international standards is crucial for businesses' scalability both within and outside the EU market.

6. The implementation period must be prolonged to at least 36 months to allow adequate time for standardisation bodies to develop the necessary harmonised European standards, provide breathing space for economic operators to comply with requirements and obligations stemming from horizontal and sectoral legislations; and to enable market surveillance authorities to set up respective institutional structures.

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

15 March 2023

CONTEXT

The exponential growth in the use of connected products is forecasted to reach twenty-nine billion[1] by 2030, hence a risk-adequate security level of these products becomes an imperative. Moreover, **the number of IoT devices across all industry verticals is expected to grow to more than eight billion by 2030**[2]. ENISA's 2022 report on NIS Investments[3] shows that **the estimated direct cost of a major security incident is EUR 200 000 on median,** yet only 30% of operators of essential services and digital services providers possessed cyber insurance in 2021 (with only 5% of SMEs subscribing to cyber insurances). These figures show that businesses are still maturing to the task of being cyber resilient, and that the playing field between bigger and smaller operators is still uneven.

Unveiled in a crucial period for the digitalisation of our economy, BusinessEurope believes the proposal for Cyber Resilience Act (CRA) aims to achieve twin-objectives: increasing cyber resilience while fostering competitiveness and innovation in the EU. Therefore, EU regulations, intended to increase the common cyber resilience, shall have a risk-based approach so that the rules do not cause disproportionate burden across sectors or across different sizes of enterprises.

Additionally, the **global gap[4] of cybersecurity talent amounts to 3.4 million experts.** Whether one needs professionals for products' designing, developing, manufacturing, or testing and assessment phases, or for enforcing the provisions of the proposed legislation – this global shortage will have an impact. Moreover, the upcoming intensive implementation of and compliance with laws already adopted in this EU legislature under the EU Cybersecurity and EU Data strategies shall not be underestimated, neither in terms of businesses' capabilities, costs, and maturity, nor in terms of the capabilities, costs, and maturity of the enforcement authorities.

BusinessEurope highlights that a legislation delivering a coherent set of harmonised cybersecurity requirements is important and welcomed initiative. It must seek synergies with soft measures, such as strengthened cybersecurity risk management procedures, adequately skilled professionals, and well-informed customers. This way products placed on the EU's internal market will not be an easy vector of attack that can jeopardise its functioning, and there will be ability to control damage in cases of a successful cyber-attack.

In the following pages, BusinessEurope outlines some positive provisions to be preserved during the legislative process of the Cyber Resilience Act, as well as some suggestions for further improvements. **As a Social Partner and a representative of 40 national industry associations across Europe, we remain committed to help increase Europe's cyber resilience.**

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[2] Ibid.
[3] European Union Agency for Cybersecurity (ENISA), 2022, NIS Investments,
[4] WEF, 2022; *To fill the cybersecurity skills gap, the sector needs to boost diversity*

COMMENTS

BALANCED PROVISIONS

BusinessEurope supports the Commission's chosen approach, which is based on the New Legislative Framework. We call on the co-legislators to preserve this already well-functioning regulatory process as it allows for covering different levels of necessary safeguards, based on the products' risk profile and their intended application.

We welcome the Commission's explanation in Recital 44 that the procedures for conformity assessments set out in the CRA aim at cross-sectoral coherence and the avoidance of ad-hoc variants. It is often the case that products are subject to various relevant Union acts, and we view very positively the provision that a single EU Declaration of Conformity can be issued in such circumstances. The flexibility for the manufacturer to apply the requirements that are relevant based on the risk assessment provides agility and future-proves the Regulation as the risk awareness evolves.

We are also positive about the intention to allow demonstration of conformity with self-assessment for most products. An innovation-driven aspect is also the exclusion of beta versions, and start-up sandboxes from the scope of the CRA.

We very much welcome the clarification in Article 16 where a substantial modification of a product done by a natural or legal person (other than a manufacturer, the importer, or the distributor) is subject to obligations. This is an important element as it leaves the choice to the natural or legal person as to how they would like to use and modify their product, and even potentially market it as a new product.

We welcome the good framework of requirements for notified bodies, notably that they must be transparent in their accreditation procedures, independent, competent, and free from conflict of interest. The proposal also caters for subcontractors and subsidiaries of those notified bodies that must fulfill the same conditions. In the interest of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators, in line with the intention in Article 37.

The delegation of power to the European Commission is granted for many important elements of the proposal to deliver an agile framework. In addition to this, the obligation to carry out appropriate consultations with stakeholders in accordance with the Better Regulation principles, must be transferred from Recital 62 to the main body of the legislative text.

Furthermore, BusinessEurope supports open market economy as this allows many European products to be sold outside the EU, as well as the opportunity for many products from third countries to be imported and allowing for diverse choice and a healthy competition. We are glad to see that Mutual Recognition Agreements with third countries concerning conformity assessments may be concluded for the products regulated in the CRA. This will facilitate trade and strengthen cybersecurity within the Single Market and

globally. Also, the Single Market relies on an effective standardization system that should be aligned with international standards to enable collaboration and interoperability and avoid placing barriers to EU's industry when doing business within and outside the Union.

BusinessEurope strongly believes that the proposal for a Cyber Resilience Act is already a very good basis for increasing the cybersecurity of products in the EU. **We urge that the above-mentioned positive elements remain unchanged throughout the negotiation process. Going forward, co-legislators must focus attention on further clarifying definitions, scope, risk categorisation, and consistency with other rules.**

SUGGESTIONS FOR IMPROVEMENTS

SCOPE AND DEFINITIONS

As already mentioned in our contribution to the Call for evidence for the CRA, we insist on having consistent definitions. In this respect, the definition of "product with digital elements" in Article 3 must be clarified; the CRA alone differentiates between four types of products with digital elements: (i) product with digital elements, (ii) Class 1 critical product with digital elements; (iii) Class 2 critical product with digital elements; and (iv) highly critical product with digital elements. It is evident that this differentiation aims at better risk categorisation, and product identification. However, in its current form it is insufficient to bring the needed clarity as to how to avoid overlaps or confusion with NLF-based regulations to be negotiated or applied in parallel (e.g., the AI Act, the Machinery Regulation, etc.).

Furthermore, Article 3(1) clearly defines "products with digital elements" as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately". However, Recital 9 specifies that the proposal **does not cover software-as-a-service (SaaS)** except "for remote data processing solutions". BusinessEurope highlights that the New Legislative Framework has not been applied to services and this NLF-based proposal should not introduce services in its scope given that evaluation of how the NLF must address the challenges posed by the digitalisation and the complexity of value chains is upcoming[5].

Additionally, it must be recalled that Directive (EU) 2022/2555 (NIS2) already provides an obligation for cloud service providers (including SaaS) to implement cyber and risk management measures, given that they are considered operators of essential services. Distributing crucial security patches to products with digital elements via the established market method of over-the-air-updates could capture remote data processing solutions, however the delimitation of CRA's scope should be clearer, so it (1) ensures the distribution of patches; (2) avoids double regulation.

[5] European Commission, 2022; https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

Furthermore, the definition of product with digital elements includes software, yet further clarification is necessary as to what is software-as-a-product. Recital 9 points at software that is designed and developed specifically for the manufacturer and that it is indispensable for the functioning of the product with digital elements. To ease the interpretation two additional definitions must be considered, e.g., "**firmware**" also known as embedded software, which renders the product functional; and **"developed software**" that is developed by the manufacturer, or for the manufacturer by a contractor, and where the developed software will be the property of the manufacturer.

An additional clarification is necessary as to the exclusion of open-source software that is not used in the course of a commercial activity. Recital 10 specifies what is to be understood as commercial activity for software, however it extends it to technical support services, which seem as an inclusion of services in scope, and as outlined above must be avoided. Whether or not to include open-source-software must be evaluated against its specificities, e.g. the development of open source software can be independent of any later application (including commercial): it is often difficult to identify the person or the entity maintaining an open-source software component; etc. The Impact assessment of the CRA only points that "the literature (…) in principle"[6] provides for distinction of commercial and non-commercial. However, to have a targeted and risk-adequate legislative action, the *practical aspect* of this distinction must be assessed. The co-legislators could therefore request such assessment and guidance for the evaluation of the CRA.

The definition of "**substantial modification**" could be better aligned with the Blue Guide and the recently revised Machinery Regulation. To this end, Recital 22 must be aligned with Article 3 (31). However, when it comes to substantial modification based on software change/update, the condition that the "changes were not foreseen in the initial risk assessment" may have chilling effect on (security) innovation and on the developing/release of new features to the product brought with a software update. It should be avoided that every software release requires the product to undergo a new conformity assessment, as this would be disproportionate burden to the developer and would delay the updates, which could be crucial, especially to increase resilience. The Blue Guide of 2022 clarifies that substantial modifications must be assessed on a case-by-case basis, but for the vast scope of the CRA this may not be technically feasible. Therefore, the Commission must issue guidance on substantial modification by a software change.

The concept of placing a product on the market **"without any known exploitable vulnerability"** is not risk proportionate**,** because maintaining a risk-adequate level of cybersecurity is a process[7]. Moreover, a product's cyber-resilience can be influenced by numerous factors, including the product's deployment environment, the development of new technologies, and by the evolving cyber-attack landscape. It must be highlighted that not every vulnerability has the same level of impact that can cause "significant cybersecurity risk" as defined in Article 3 (36). In line with OECD findings **"***there is no*

[6] Impact assessment, Cyber Resilience Act, European Commission, 2022, Part 2, p.30

[7] Confindustria does not agree with the text reported. According to Confindustria, to ensure adequate levels of cybersecurity, it is fundamental that are placed on the market only products without known vulnerabilities and equipped with tools/technologies to manage emerging vulnerabilities, as requested by the objectives of the European cybersecurity certification schemes defined in the Cybersecurity Act.

way to eliminate all vulnerabilities. While addressing vulnerabilities is essential, fixing all vulnerabilities would not be a realistic objective, for many reasons including cost and technical feasibility.[8] Therefore, CRA's rationale should be to minimise cyber incidents by remedying the critical vulnerabilities (scored according, for example, to the globally recognised CVS system).

In addition, co-legislators must devise a solution for keeping secure the products that are kept continuously on the market, and a method via which these products could be kept free of exploitable vulnerabilities. The option that such products are withdrawn at the moment an exploitable vulnerability is found, can be a significant drawback from a sustainability perspective; unused IT devices would have to be taken from the market, transported, and in some cases even be destroyed. The impact assessment does not provide any cost-benefit evaluation in such situations. Therefore, we advise against this option.

A suggestion for a solution is to amend Annex I Section 1 (2) in such a way, that it directly references the vulnerability handling process of Annex I Section 2. In other words, products with digital elements that have a vulnerability, but for which an update is available, and which can be immediately installed at the time of their first use, should be kept on the market, instead of disproportionately recalled. This way potential buyers of such products will not suffer unnecessary shortages or overall product unavailability. Furthermore, to aid the potential buyer to securely initiate the product and patch the vulnerability, there must be an effective information exchange and possible assistance available.

RISK CATEGORISATION AND CONFORMITY

There is need for further improvement of the risk categorization. For instance, according to the proposal IoT industrial applications are always viewed as critical, but some IoT products in practice may not be. A better way of addressing this aspect of the proposal is if the co-legislators focus on the intended use of products. This is necessary because one product can perform a more critical or a less critical function depending on the specific application environment. For example, from industry's point of view, it makes a substantial difference with regards to the criticality of the same microprocessor whether it is used within a coffee machine or a router.

While dealing with risk categorization and the respective obligations, co-legislators must also bear in mind that it is out of the control of the manufacturer to monitor which applications a product might ultimately fulfill (e.g., industrial or consumer), especially, when the product is sold by an importer or a distributor.

It must be noted that the wide array of products in scope of this legislation as well as the number of economic operators covered, the capacity for a third-party conformity assessment may be significantly diverging. Furthermore, there is a risk that the manufacturers of Class 2 critical products, who must undergo 3rd-party assessment, could see significant delays in acquiring proof of conformity due to potential bottlenecks

[8] OECD,2021, Encouraging Vulnerability Treatment Overview For Policy Maker, page 12

in the notified bodies for the lack of trained cybersecurity experts and controllers (as mentioned above, a global gap of cybersecurity experts is estimated at 3.4 mln people).

Inconsistent enforcement or bottlenecks could potentially discredit the trust in the very market rules the CRA is aiming to set. This would cause a *lose-lose* situation: for the business as they would face administrative burden; and for administration as they would be faced with unmanageable workload.

A possible solution to this situation could be if the list of critical products outlined in Annex III is revised to reduce its scope, by considering the intended use of the products. An additional criterium that could be considered is whether the product is controlled remotely or locally, as devices that are controlled remotely tend to be riskier and may in some cases warrant a third-party conformity assessment.

The **highly critical products** for which the conformity assessment would be a mandatory certification will only be defined via delegated act. **In practice, this would mean that the scope of the CRA regulation will not be fully clear at the time the regulation is adopted.**

This scenario brings uncertainty for both: manufacturers potentially applying one conformity assessment procedure until the delegated act comes in force (requiring certificate under EU cyber scheme); and authorities and their obligation which products to monitor for compliance. **BusinessEurope urges the co-legislators to amend the CRA proposal in such a way as to ensure that the highly critical products are outlined in a *lex-specialis*** after a thorough impact assessment.

We highlight that Article 54(3) of the Cybersecurity Act (CSA) allows for the possibility that schemes be employed to demonstrate conformity with another legal act, “in the absence of harmonised Union law”. This option is provided to the Member States, (not delegated to the Commission). Hence, it must be Member States-driven initiative that schemes are made mandatory because a harmonised Union law is missing. Recital 4 of the Cyber Resilience Act confirms that the very intention of this proposal is to be the harmonised Union legal act for cybersecure products placed on the EU market. This is another argument that the highly critical products (requiring mandatory certification scheme) must be defined in a *lex specialis* adopted by the co-legislators if there is evidence that the harmonised rules of CRA do not deliver effective results for some products. Any future legislation must absolutely avoid the risk of duplicating the conformity assessments requirements.

Recalling BusinessEurope’s contribution to the CRA Call for evidence and to ensure legal certainty and harmonisation of the internal market **the cybersecurity requirements in harmonised European standards developed and aligned with international standards must be the dominant conformity option to deliver the scale for doing business across borders and internationally**.

European and national legislators are currently implementing or yet to transpose a multitude of measures in the cybersecurity rules (NIS2, DORA, sector specific rules). Moreover, within the foreseeable future product-specific cybersecurity certification schemes, stemming from the Cybersecurity Act [e.g., the EU Cloud Scheme (EUCS);

EU 5G Scheme (EU5G)], will also come into play. **It is of high importance, therefore, to avoid any kind of regulatory overlaps and inconsistencies.** To this end, we strongly recommend that ENISA and the European Commission limit the development of new cybersecurity certification schemes under the Cybersecurity Act to the absolute minimum necessary.

Even though the development of **common specifications in Article 19** is intended as a fall-back measure**, the necessity at this stage** to have such an option at all within the first horizontal legislation on cybersecurity requirements for products **is not evident**. Deleting this option will be a signal by the co-legislators that requires the market to develop standards that will be agile and outcome-oriented in view of complying with the horizontal requirements of this Regulation.

CONSISTENCY WITH OTHER LEGISLATION

We recall our request that the Cyber Resilience Act must **avoid ambiguity and the placing of more layers of complexity of cyber requirements for a given product:** one product, given a specific application, should be covered by one set of cybersecurity requirements.

We note the intention of the Commission to streamline compliance, however, it will take great coordination effort for the EU executive and for the respective negotiation teams in the EP and in the Council, to maintain essentially equivalent to the CRA requirements for products in particular with the ongoing AI Act, but also with recently concluded GPSR, DORA, Machinery Regulation, etc.

We find this approach complicated and vulnerable to changes, therefore we would like to see that only the CRA is the framework applicable for the overlapping products in scope of either of the abovementioned files. Moreover, **any new *lex specialis* should always be built on the same principles as the Cyber Resilience Act, and clearly state and justify the additional requirements.**

CRA AND RED DELEGATED ACT

We view positively the intention stated in the CRA with regards to the withdrawal of the RED Delegated act. We support very much that this is clearly stated in the legislative text. In addition, the efforts already undertaken for the standardisation request for the RED Delegated Regulation must not be discarded but considered. To support the smooth transition between the two instruments, BusinessEurope insists on the introduction of a transition period and a grace period for products falling in the scope of both the CRA and the RED Delegated Act. This will lead to more certainty for manufacturers and will avoid unnecessary legal costs.

CRA AND NIS2 DIRECTIVE

BusinessEurope appreciates that the CRA includes reporting mechanisms that will eventually lead to more timely remedies for the affected products. However, it must be

stressed that any reporting should not be a burdensome exercise, as gathering information is time-consuming. Incident handling and mitigation must have a priority. We urge co-legislators to align the periods for reporting with those under the NIS2 Directive, and the GDPR to 72h.

When it comes to vulnerability notifications, it must be underlined that a vulnerability can be actively exploited for months without the manufacturer being aware of it; or a vulnerability may be identified months after an incident had occurred. Therefore, more alignment is necessary with the NIS2 Directive, especially considering the upcoming vulnerability database of ENISA, the voluntary vulnerability disclosure provided in the revised Directive; and the information in the final report after an incident, which too will outline what vulnerability led to it. **By no means should businesses be obliged to report several times the same information**.

The primary goal for EU's cyber resilience efforts should be to support market players and allow for a timely mitigation of an incident or an actively exploited vulnerability by a malicious actor that poses significant cyber risk.

To fulfil its security objectives, the CRA should therefore find the right balance to effectively allow for the necessary information sharing between manufacturers and surveillance authorities, hence, to avoid placing unnecessary cyber risks to products disclosing unpatched vulnerabilities should not be required.

Furthermore, the obligation for vulnerability reporting must be risk-based and proportionate too. The vulnerabilities that are "actively exploited by a malicious actor" and "pose a "significant cyber risk", and are "a high risk to the functioning of the internal market" should be the ones that absolutely have to be reported within a reasonable timeframe, e.g. 72h. The remainder of the identified vulnerabilities should be reported in bulk, e.g. once every two months. This way the risk to the internal market is minimised and at the same time the database for vulnerabilities will be filled in, thus allowing for an adequate vulnerability scoring system to be applied (such as the CVSS). This approach will additionally help importers and distributors for whom it may be rather difficult to assess whether a detected vulnerability is critical or exploited and thus whether it is under swift reporting obligation or not.

Manufacturers of products with digital elements should only have to report once within the EU. The co-legislators should urge ENISA and the Commission for the establishment of a fully digital information flow and secure reporting mechanism and allow for the information to flow from CSIRTs to market surveillance bodies and ENISA. **Due to the massive gap in cybersecurity professionals, efficient reporting mechanisms based on the once-only principle are crucial to ensure that companies can focus on incident and vulnerability handling**.

As part of the concerted efforts for cyber resilience, the recently adopted NIS2 Directive Recital 62 and Article 12 provide that competent authorities of Member States and CSIRTs, as well as any other entity that does not fall in the scope of NIS2 (e.g. government security agencies) could alert vulnerabilities in the European Vulnerability Database managed by ENISA. This kind of voluntary cooperation becomes

indispensable for the manufacturers to be able to verify against that database what vulnerabilities are discovered for their products and essentially to fulfill their obligations.

TECHNICAL DOCUMENTATION

Software bill of materials (SBOM): Recital 27 reads: "In order to facilitate vulnerability analysis, manufacturers should identify, and document components contained in the products with digital elements, including by drawing up a software bill of materials. … It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties." The SBOM is a powerful tool in the hands of customers to understand any exposure to vulnerabilities of components used by the manufacturer of the product. Without it, on the one hand, blind exposure to vulnerabilities would remain and, on the other hand, it would not be possible to easily control the work of manufacturers in terms of fixes and remedies.

While we acknowledge the necessity for meaningful transparency, we underline that SBOM should be disclosed when the market surveillance authorities request them in order to fulfil their legal obligations; and leaving the rest to manufacturers to choose whether or not to make this information available to customers.

In fact, SBOMs have not reached the required maturity level on how should be implemented, shared, and used, so that it warrants a regulatory intervention. Instead of implementing act according to Article 10 (15), co-legislators must request guidance from the Commission, considering the ISO/IEC 5962:2021 and Cyclone-DX where SBOMs are addressed.

MARKET SURVEILLANCE

BusinessEurope views positively that the proposal extends the application of Regulation 1020/2019 and that market surveillance legislation will apply to products covered by the CRA. The proportionality element of the fines must be considered given the overall risk-based approach of the proposal. A necessary clarification is that an economic operator should only be fined under one regime. It must be recalled that typically cost of compliance, especially for SMEs, is relatively more significant.

According to the proposal the Commission is empowered to order market surveillance activities to be carried out by ENISA in exceptional circumstances: the Commission can ask ENISA to carry out evaluations of products and based on the information/findings provided by ENISA the Commission takes measures, including recalling of product.

BusinessEurope questions this approach, as the mandate of **ENISA,** set out in the Cybersecurity Act, is clear that the Agency shall act independently **"while avoiding the duplication of Member State activities and taking into consideration existing Member State expertise."** (Art 3 (3), CSA). **It is not evident how and when ENISA developed the necessary capabilities** that exceed the ones of Member States' market surveillance authorities, and how no duplication of activity will be ensured.

Furthermore, market surveillance authorities are expected to increase capabilities and resources to match their responsibilities under several revised product-related laws that

will come into force in the next years (Machinery Regulation, GPSR, sectoral laws, etc.). Market surveillance authorities must be given the opportunity to build capacity and synergies as many of the products will be, in fact, overlapping.

APPLICATION TIMELINE

The broad and comprehensive nature of the CRA has far-reaching implications for its implementation. Put in perspective, during the current application timeline set in the proposal, i.e., 12 and 24 months:

- Harmonised European standards must be developed (either from scratch or based on IEC 62443, and an alignment with the work already undertaken on the standardisation request for the RED Delegated Regulation should take place).
- Industries must implement the essential requirements across all products with digital elements according to Article 2 (1);
- Companies across sectors and with different level of cyber maturity
    - have to review their internal measures to ensure CRA-conformity / or to set up respective measures;
    - have to implement a vulnerability handling mechanism that accommodates the requirements set out in Annex I Section 2;
- Member States must organise the market surveillance outlined in Article 43 (including by updating organisational structures and hiring new employees);

It is evident from the points above that the application period must be prolonged. During the current multiple crises faced by private and public sector alike and considering the cumulative effect of different pieces of regulation adopted in this EU legislature, **we urge the co-legislators to provide breathing space for businesses and to prolong the period to at least 36 months before the CRA becomes applicable.**

****

FURTHER CONSIDERATIONS FOR CYBER RESILIENCE

As outlined above cyber resilience is a holistic endeavour. It is not only a matter of regulating the private sector more, but politics must also address the increased threat. The private sector must not be made solely responsible for defending itself against state threat actors. Furthermore, to ensure that manufacturers of products with digital elements are made aware of all known vulnerabilities, BusinessEurope urges the European co-legislators to require government bodies – both at supranational, national and regional level – to share their knowledge of vulnerabilities, i.e. backdoors, with the respective manufacturer and refrain from legislation that allows exploitation of vulnerabilities in order to break or circumvent encryption.

Vulnerabilities are a security risk for all, and they weaken Europe's cyber-resilience. Henceforth, the Cyber Resilience Act can only achieve its intended goal if both manufacturers and government bodies contribute their fair share. Such an obligation should be introduced in a separate piece of legislation by Member States and should come into effect not later than at end of the implementation period of the Cyber

Resilience Act. Resilience is something that the industry is continuously seeking, and it must be ensured that the debate does not develop into security against innovation, placing tougher rules but not necessarily achieving resilience.

Additional and very important point is that the Regulatory Scrutiny Board highlights that the cost-benefit analysis of the impact assessment of the CRA proposal "is incomplete". BusinessEurope echoes this concern. There is no estimation, for example, as to how many (new) employees (on average) will be needed in the private sector to make sure the CRA requirements are met. There is also no analysis on how much the increased cybersecurity protection and subsequent maintenance will impact the prices of the products placed on the market. Complex products involve complex testing to secure that the complex system functionality is maintained after security patching, and it is hard to define the cost to include in the initial price.

The impact assessment report also lacks a more targeted estimation of the impact on the relationship of SMEs with manufacturers of hardware components from third countries and the cost implied to make these producers compliant with the new CRA requirements, and whether there will be a relative increase of the cost of doing business for SMEs.

The absent estimation of the above-mentioned aspects for the private sector is a significant shortcoming for such a horizontal and ambitious proposal. We encourage the co-legislators to commission a study evaluating and addressing the financial impact of the proposal on the private sector, so there is an informed legislative decision-making to the highest extent possible.

This approach will also help Europe's competitiveness, especially taking into consideration the global geopolitical and economic tendencies, which inherently affect the European business climate. It must be avoided that in these circumstances *European* regulation slows down the *European* industrial digitalisation by introducing compliance requirements for a vast array of products without the necessary cost-benefit analysis.