BusinessEurope's contribution to the Call for evidence on Cyber resilience act

Over the years BusinessEurope consistently called for encouragement of all players in the value chain to ensure products, processes and systems are cybersecure from the earliest stage of the engineering process in a dynamic way, thereby also promoting responsible innovation through security-by-design. A one-size fits all approach would not adequately meet the requirements of the various existing risk scenarios, and especially in an Industrial IoT environment. BusinessEurope advocates for balancing the allocation of responsibilities of different economic operators in the value chains.

- The Cyber Resilience Act (CRA) should take **a market-driven approach** and recognise how all sectors and sizes of businesses currently understand and focus on identifying, assessing, and addressing cybersecurity risks in their products, processes and systems. The ambition of the EU legislation should be to develop 'Zero-trust' approach that boosts the level of protection against external actors.
- When developing the Cyber Resilience Act, the European Commission should introduce horizontal cybersecurity requirements based on the **New Legislative Framework** independently of products group. The technical specifications to meet the cybersecurity requirements under the CRA should be laid down in harmonised European standards, which are to be applied as part of conformity assessment. Where necessary, third-party conformity assessments would be appropriate for certain category of high-risk products.
- To ensure cyber resilience, the **requirements should specify dynamically** the organisational and technical procedures the manufacturer or provider has to put in place to effectively and timely **react to new threats and challenges**.
- **CRA** should be **lex generalis** when it concerns baseline cybersecurity requirements for connected products.

As a Social Partner and a representative of 40 national industry associations across Europe, **BusinessEurope remains committed to increasing Europe's cyber resilience.** Below we outline some concerns and suggestions to be considered in the upcoming proposal:

Concerns:

- **Avoid fragmentation with other legislation.** The proliferation of cybersecurity requirements in different legislative initiatives over the past years (e.g. the General Product Safety Regulation; the Machinery Directive; the Delegated Regulation under the Radio Equipment Directive; the NIS2 Directive; the Digital Operational Resilience Act; the AI Act; certification schemes under the Cybersecurity Act; national cybersecurity initiatives) increases the risk of having multiple and possibly conflicting requirements for the same products or economic operators. The Cyber Resilience Act must bring legal clarity, ideally, by introducing horizontal cybersecurity requirements based on the NLF, and additionally stating which *lex specialis* requirements continue to prevail.
- **Avoid placing more layers of complexity on cyber requirements for a given product.** One product given a specific application should be covered by one set of cybersecurity requirements.
- **Avoid disproportionate burden on businesses.** The Cyber Resilience Act must take a holistic view on the cybersecurity ecosystem and address the variety of actors that may impact a products' security during its lifecycle. Private users and governments must assume their respective responsibilities, to contribute to an enhanced cybersecurity and resilience through

cyber hygiene, appropriate trainings, and secure processes. Moreover, governments across the EU should share their knowledge of vulnerabilities in digital products to facilitate a speedy development of updates and patches.

Suggestions:

- The **New Legislative Framework is best equipped** to strengthen the cyber resilience of products, and can be adapted for processes, and systems in the EU. It allows for covering different levels of resilience based on the products' risk profile and their intended application. It must be taken into account that in IIoT setting many of the products have embedded software or there is a software that can be installed later to render the product operational. Therefore, all products and (embedded or to be embedded) software as a product within the scope of the CRA proposal should be put on the market/put in first use once it has been acknowledged that they are free of known exploitable vulnerabilities. (Whenever relevant vulnerabilities emerge after the placing on the market, update mechanisms should be provided as well as a specific process to make the necessary corrections, according to established market best practices). **For many years now the CE mark** has established its reliance, demonstrating conformity with EU rules, and providing confidence for private and commercial customers.
- Ensure that **definitions** used throughout the CRA are aligned with the existing legislation and are sufficiently precise. It must be noted that products, designed for B2C and B2B markets, have different lifecycles, operational environment, capacities, potential risks and intended uses, which would affect the risk categorisation. It is important to note that in a B2B environment products are integrated into highly complex systems, hence these interactions must also be accommodated by the CRA.
- **Coherence between the Cybersecurity Act and the Cyber Resilience Act**: Horizontal requirements in CRA and schemes under CSA (Title III) must be coherent and not contradict each other. To ensure legal clarity the horizontal cybersecurity requirements in a harmonised standards must prevail if there is a conflict between the CRA and another (existing) legislation. However, it is also noteworthy that Article 54(3) of the Cybersecurity Act allows for the possibility that schemes under CSA can be employed to demonstrate conformity with another legal act. Conflicts between standards and schemes must be avoided in order to facilitate legal clarity and compliance. Moreover, the CRA shall not declare the voluntary schemes as mandatory.
- **International dimension:** The international recognition and compatibility of EU cyber resilience requirements is key. The Single Market already relies on an effective standardization system (with CEN-CLC/JTC 13; ETSI TC CYBER, etc.). It will be critical to continue engaging with industry for the development of common technical specifications. Harmonised European standards should leverage existing international standards to allow for global market access and decrease costs for businesses in the EU. The CRA should strengthen the principle of "one standard, one test, accepted everywhere".
- **Strengthen the market surveillance**: Sufficient and effective market surveillance is essential to ensure compliance. Hence, the CRA must ensure that authorities have the necessary competences, to be able to competently commission and/or carry out tests, so only products that meet the relevant requirements are on the market.