Charter of Trust's comments on the EU Cyber Resilience Act

Introduction

We, the members of the Charter of Trust, welcome the current policy negotiations taking place around the European Commission's proposed EU Cyber Resilience Act (CRA). Digitalization has transformed nearly every aspect of modern life. Today, billions of devices are connected through the Internet of Things. While this created great opportunities, it also potentially harbors great cybersecurity risks. To make the digital world more secure, we have joined forces as the Charter of Trust - a unique initiative by leading global companies - with a cooperation that has reached significant milestones toward improving cybersecurity and has ambitious goals for the future. The Charter of Trust's focus is on three important objectives: To protect the data of individuals and companies; to prevent damage to people, companies, and infrastructures; and to create a reliable foundation on which confidence in a networked, digital world can take root and grow.

Our view

The Charter of Trust welcomes the Commission's proposal for horizontal rules introducing cybersecurity requirements for connected products. We believe that improving products and software development practices and transparency will benefit the entire cybersecurity ecosystem.

Our partners support the need for all organizations to adopt the highest appropriate level of security and data protection practices by default: similar to rules related to energy labelling and eco-design set as common EU wide minimum standards, the CRA's overarching goal should be to ensure a high level of consumer and industrial protection when connected products are placed on the EU market.

The CRA provides an opportunity for the EU to adopt clear, harmonized rules following a risk-based approach and which avoids inconsistencies with other EU legislation. Indeed, the EU has already adopted many existing regulations in the digital domain. Policymakers should thus ensure seamless and clear application between the CRA and other product-related and cybersecurity legislations[1] to provide more legal certainty to businesses across the supply chain.

To achieve these objectives, the Charter of Trust calls on EU policymakers to clarify the following issues in the CRA:

1- Limit and clarify the scope:

The definition of *"products with digital elements"* needs to be better defined, so that requirements clearly apply to "products" and not "services". Indeed, the idea of including *"remote data processing solutions"* in the definition of products with

[1] European Cyber Security Act (CSA), Radio Equipment Directive (RED), Machinery Directive (MD), General Product Safety Directive (GPSD), General Data Protection Regulation (GDPR), revised Network and Information Security Directive (NIS 2), as well as the upcoming AI Act and the revised Product Liability Directive

digital elements may inadvertently include cloud services in scope such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS). Those services are already subject to cybersecurity and risk management requirements as "essential services" under the NIS 2 Directive and should thus be more clearly excluded from the scope in the normative part of the proposed Regulation: this could be easily achieved through **scoping down the definition of remote data processing to cases when it is essential for achieving the product's primary function**.

We would also call on policymakers **to exclude "hardware" in the notion of "remote data processing**", as this may cover the underlying infrastructure on which cloud operates, which provide no security benefits to the CRA's overarching goal of increasing consumer and business user protection.

Finally, we believe that **spare parts should be exempted from the CRA**: OT environments and critical infrastructures usually have an extended lifetime (30+ years). For legacy products used as spare parts, it is very often not possible to bring them in conformity with the current state of the art as required by the EU CRA. For newly developed spare parts, which need to fulfil the new EU CRA requirements, not necessarily all compatibility requirements with the legacy system can be achieved.

2- Establish a review process with manufacturers to classify a product as "critical":

We regret to see that **the EU's chosen approach to determine whether a product is deemed critical will in fact undermine the CRA's risk-based approach**: as currently drafted in Article 6 and in Annex III, a whole range of products would end up in the highest risk category despite the proposed Regulation's clearly stated objective to *"only include a narrow share of the market"* in this category.

We welcome the Council's proposal to reduce the list of critical products in Annex III, and encourage the co-legislators to adopt a phased approach by starting with a manageable list of highly critical products.

Additionally, the Charter of Trust calls on the legislators to make the review process to determine whether a product is critical, more transparent and inclusive, engaging wider range of stakeholders including manufacturers. We suggest that this review process should consider product's risk environment, including its specific and intended use and application, as defined by the manufacturer. In cases of general-purpose technologies, the obligation should be on the customer to set out their requirements to match their context of use.

This approach would ensure that relevant products would be subject to optimal cybersecurity requirements, which would ensure that organizations and manufacturers to adequately distribute their resources and ensure that they focus on tackling real risks.

3- Vulnerability handling and reporting rules should be in line with international best practices:

The CRA's proposed obligation in Article 11 to report *"actively exploited vulnerabilities"* in no more than 24 hours means that there would be a clear risk from disclosing unpatched or unmitigated vulnerabilities, if this extends to users as well, thus undermining the very purpose of the CRA. Besides, from a supply chain perspective it is not always feasible to reach all users directly. Moreover, the proposed timeline would be inconsistent with the incident reporting obligations under NIS 2. Manufacturers should focus primarily on handling vulnerabilities, whilst informing the relevant authorities, and sharing this information with users, once mitigation guidance/patches are available, in line with any existing international best practices, such as those from CISA.

Moreover, the CRA's proposed requirement to deliver products ***"without any known exploitable vulnerabilities"*** is an impossible bar to set. A product's security can be influenced by numerous factors, including the product's deployment environment, the development of different technologies, and by the evolving cyber-attack landscape. Such a requirement would discourage manufacturers from conducting meaningful security testing, potentially leading some to avoid scanning products (this way, keeping those potential vulnerabilities "unknown"), and thereby leading to less secure products being delivered on the market. Additionally, some vulnerabilities, either due to how components may be integrated into the product with digital elements or due to compensating controls, are not actually exploitable within the context of that product. A manufacturer, in appropriate circumstances, should be permitted to document those reasons for not remediating such a vulnerability.

4- Leverage existing international security standards:

International standards are the result of broad stakeholder consensus, reflect the best practices of the industry and are constantly updated to keep pace with the ever-evolving threat landscape: maintaining a harmonized approach to cybersecurity regulation helps improve security for all by reducing the risk of cyberattacks and ensuring that all stakeholders are held to the same high standards. It also facilitates trade and cooperation among countries, reducing the potential for a fragmented and ineffective approach to cybersecurity. Since many organizations already comply with one or more of these standards, their use would facilitate both standards development and compliance.

The EU has an effective standardization infrastructure (with CEN/CENELEC, ETSI), and **it will be critical to continue to closely engage industry in strategic committees** for the development of cybersecurity standards, certification schemes, or conformity assessment criteria that are yet to be developed. **The Charter of Trust stands ready to engage with EU regulators in this area.**

5- **Prioritize cybersecurity workforce development:**

Europe’s cyber-skilling efforts need to keep pace with the growing demand for cybersecurity professionals in both the public and the private sector. This not only jeopardizes industry compliance efforts but also adequate enforcement of the proposed cybersecurity regulation. A detailed implementation roadmap should account for these challenges, include efforts to increase readiness and ensure that ENISA, conformity assessment bodies and market surveillance authorities have the ability to fulfil their responsibilities.

6- **Allow economic operators a longer transition period or a phased approach to comply with the new rules:**

While initial enforcement can be based on self-assessments, many new obligations in the proposed CRA are based are yet-to-be developed cybersecurity standards, certification schemes, conformity assessment criteria or delegated acts, effectively not allowing manufacturers to start planning at this stage.

The CRA should allow for a significantly longer transition period (of at least 48 months) or consider a phased approach in order to enable businesses to fulfil their obligations, allowing sufficient lead time to incorporate requirements into the design and development of products. This would help to better consider the entire ecosystem and supply chain (customers, suppliers, OEMs) and to better respect the standards’ development processes.

Contact the secretariat of the Charter of Trust:
contact@charteroftrust.info

Website: www.charteroftrust.com
LinkedIn: https://www.linkedin.com/company/71503604/admin/feed/posts/
X (formerly Twitter): https://twitter.com/charteroftrust