ETNO-GSMA position paper on the Cyber Resilience Act

BACKGROUND

The Cyber Resilience Act (CRA) proposal comes at a time when European society, its citizens and businesses have been dealing with a crisis period marked by the COVID-19 pandemic and the war in Ukraine. The telecommunications sector has been capable of responding to these challenges and of demonstrating its robustness, by providing secure and reliable infrastructures and services that are essential for the functioning of the EU's Digital Internal Market. However, telecommunication network operators are still faced with security gaps in their digital value chains that need addressing.

The number of connected devices marketed in the EU has risen exponentially in the past years and is expected to continue to do so. Newer generations of connectivity and the maturing of 5G networks will enable the rapid growth of the Internet of Things (IoT): the number of active IoT connections in Europe is expected to reach 370mn in 2023, up from 204mn in 2021, and is forecasted to reach 770mn by 2030[1]. This will broaden the threat landscape significantly, demanding more efforts and investments by operators to protect their infrastructure and users.

- According to the CRA Impact assessment, the main attack vector for security breaches is the exploitation of vulnerabilities in hardware and software. The share of incidents resulting from exploits against weaknesses in the computational logic and design of software range from 62% for operators of essential services under the NIS Directive to 90%.
- According to the ENISA Telecom Security Incidents Report 2021, the most frequent root cause of telecom security incident reports is hardware failures (18%) followed by faulty software changes/updates (16%) and software bugs (15%).

At the same time there are limited incentives other than reputational risk for companies to properly address security, especially in the enterprise market. Whilst critical infrastructure providers such as telecoms are already subject to stringent security rules, providers of hardware and software are not fully covered by the current EU policy and regulatory framework, thereby leaving gaps and increasing the vulnerability of the entire ecosystem.

For operators of critical infrastructure, it is paramount to ensure network and service resilience through a better allocation of responsibility for cybersecurity along their value chain. Vendors of digital products that become an integral part of the critical services delivered to end-users are often best placed to manage their own vulnerabilities, and thus to address cyber threats related to their own products in the first place. Clear mandatory requirements for hardware manufacturers and software developers to manage and mitigate cybersecurity risks would greatly enhance the level of security and robustness of digital products used in telecom networks and services.

Therefore, we welcome harmonised cybersecurity requirements for digital products in the proposed CRA, which can bridge the regulatory shortcomings in cybersecurity responsibility and liability cascading in several sectors. It is critical that the CRA improves the cybersecurity of digital products in business-to-business (B2B) environments, particularly of those products that are employed in the critical functions of users that operate in critical sectors.

[1] State of Digital Communications 2023 Report, ETNO.

KEY RECOMMENDATIONS

ETNO and GSMA recommend that the final CRA regulation meets the key objectives that have been pursued by the initial proposal:

- Apply horizontal rules covering the entire supply chain so as to ensure regulatory coherence, consistency and end-to-end security in the supply chain;
- Follow a risk-based approach to keep the framework proportionate and manageable for the various actors in the supply chain, since not all devices/software bear the same risk;
- Ensure that products, especially software, are built secure-by-design and remain secure throughout the lifecycle;
- Implement robust market surveillance capabilities to enforce the rules;
- Promote a level playing field between European and non-European competitors.

In light of these objectives, we recommend that co-legislators make some relevant changes to the draft regulation to effectively enhance the cybersecurity of products and services and the cyber resilience of the internal market:

- Improve the harmonization of the whole cybersecurity legislation in Europe, by introducing uniform concepts and definitions that would also supersede unclear or diverging notions in other relevant pieces of law.
- Make a clear distinction between networks within the scope of the NIS2 Directive and products with digital elements within the scope of the CRA. Specify clearly that electronic communications networks (ECN) are explicitly excluded from the scope of the CRA. ECN providers use products with digital elements supplied to them by third-party manufacturers to ensure a resilient and secure functioning of their networks. Under the CRA, manufacturers of these products must remain directly accountable and responsible for the security of those products, from conception and throughout their lifetime.
- Ensure that all products with digital elements that can be used for the security critical functions of an ECN are listed in Annex III.
- Further strengthen the risk-based approach, recognizing the differences between consumer and enterprise products and modulating the obligations for economic operators according to the different criticality of products.
- Keep Software-as-a-Service (SaaS) in scope of the CRA, as it is increasingly an integrated part of digital products and networks.
- Maintain the view that open-source software developed or supplied outside of a commercial activity should be firmly excluded from the proposal, but clarify that, when an economic operator monetizes and places a product that integrates open-source software on the market, that operator is responsible for the product, including updates, throughout its lifetime.
- Ensure that manufacturers support their products throughout the product-specific expected lifetime, whatever it might be, not a fixed number of years. All known vulnerabilities must be fixed in accordance to their risk level, without undue delay. Provide for responsible disclosure of known exploitable vulnerabilities, based on established norms and practices such as the Common Vulnerability Scoring System.
- Keep the reporting obligations proportionate to the risk so that they support a secure supply chain rather than hinder its functioning. This includes aligning requirements with the process, scope, and organizational setup of the notification requirements under the NIS 2 Directive.
- Strongly promote the use of existing international standards and use common specification only as a last resort.

We elaborate on our recommendations in the next sections of the paper.

SPECIFIC ISSUES

Scope

Clarification of the Scope

The scope of the CRA is very wide. The CRA is clear about the intention of the law to support Electronic Communications Network (ECN) providers – as well as other entities in critical sectors regulated by the NIS 2 Directive – in their compliance efforts. Nonetheless, to avoid any ambiguity, ECNs should be explicitly excluded from the scope of the CRA. An ECN is a digital infrastructure, not a final product with digital elements as such, and ECN providers use products with digital elements provided to them by third-party manufacturers to ensure resilient and secure networks.

Network parts are manufactured with the intended use of building and operating a network; therefore, the manufacturers of these products must remain directly accountable and responsible for the security of their products from conception and throughout their lifetime. All products with digital elements that can be used for the security critical functions of an ECN should be listed in Annex III.

Open-Source Software

It is imperative that free and open-source software, when developed or supplied outside of a commercial activity, be clearly excluded from the scope of the CRA. In particular, it would be important to clarify in Recital 10 that, when open-source software is integrated into a final product that is commercialized and/or proposed together with services and placed on the Single Market by an economic operator, then the responsibility for this final product or the proposed open-source software throughout its entire lifecycle shall be on the economic operator that has placed them on the Single Market.

Software-as-a-Service

Telecommunication providers can use SaaS to access on-demand the applications they need to run their services and networks from the cloud, on a subscription basis. They can move various functions to SaaS, ranging from analytics, to security, to core network functions. SaaS underpins network functions virtualization (NFV), which virtualizes network processes that were traditionally run on hardware devices such as routers, switches, firewalls, and load balancer.

We support the inclusion of SaaS in the scope of the regulation, as the secure provision of SaaS integrated or interconnected with a digital product is becoming increasingly essential to determine the cyber resilience of a that product. For the sake of legal certainty, we recommend streamlining the CRA scope in accordance with the proposed Directive on liability for defective products whereby *"software is a product (…) irrespective of the mode of its supply or usage, and therefore irrespective of whether the software is stored on a device or accessed through cloud technologies".* As SaaS is increasingly becoming an integral part of telecommunication networks, the CRA should not leave any gap in supply chain security.

Obligations of manufacturers

Role of manufacturer

As already mentioned, clarity of roles within the supply chain is particularly crucial for the critical entities regulated by the NIS 2 Directive, which need to fully understand their obligations deriving from both laws. It would be necessary to better clarify when a distributor or importer qualify as a manufacturer under the CRA, according to Art. 15.

For instance, it is unclear to what extent does 'marketing under own name or trademark' turns a company into a manufacturer. Under the NLF, some national competent authorities have applied nuanced, divergent interpretations that may differ from the Blue Guide on the implementation of the product rules.

Risk-based approach

We welcome that the essential requirements in Annex I are the same for all products and very much support the suggested risk-based approach.

It would be valuable to include the security capability determined by the conformity assessment, as well as the assumptions made in the risk assessment, in the information to the user requested according to Annex II. Then the user can make an informed choice and the manufacturer will remain accountable for the proper functioning of the product according to the capability they claim.

We support that the mechanism of demonstration of conformity with the security requirements must be sensitive to the criticality of the product, in order to provide users of critical products with an extra layer of assurance. We stress however that the conformity assessment and certification processes for critical and highly critical products should not cause delays in the rollout of 5G network infrastructure, bar the risk of hampering the timely transfer from older network generations and the upgrade to new technology.

Responsible vulnerability disclosure

We agree that a product with digital elements should be delivered without known exploitable vulnerabilities that entail a high risk for the product and its users. Disclosing vulnerabilities has to be done with caution and in a way that the risk of exposure does not increase, thereby leading to further security incidents (typically when a reliable fix is not readily available and not possible to implement). We would therefore caution against immediate public disclosure of vulnerabilities, with the exception of those vulnerabilities with known exploits and available fixes that should be disclosed at the very earliest to avoid further harm. This does not prevent the mandatory, timely and safe private sharing of vulnerabilities – even before a fix is available – between trusted stakeholders in the private and public sectors who can help to mitigate the vulnerability, where immediate public sharing is not appropriate to allow for the necessary remediation to be planned and implemented.

Against this background, it is crucial that the regulation defines the "known exploitable vulnerability" with a high severity that should be disclosed, according to the Common Vulnerability Scoring System (CVSS). Furthermore, for the sake of regulatory harmonization, the baseline definition of vulnerability should not only be aligned with the NIS 2 Directive, but also with the scope of Regulation (EU)

2019/881 to cover vulnerabilities in ICT processes. In fact, a vulnerability can also arise from a weakness of flaw in a software coding, configuration, or update.

The Product Lifecycle Approach

The manufacturer's responsibility to comply with the essential cybersecurity requirements and reporting obligations laid down in the CRA are closely related to a product's life cycle. The CRA should clarify the meaning of "whole life cycle" and "expected product lifetime" in the context of this regulation, and how end-of-life equipment should be handled.

Article 10(6) of the current proposal places a five-year limit for manufacturers to keep handling the vulnerabilities of their products.

We recommend that the regulation abstains from setting a fixed deadline (i.e., five years) to the duty of manufacturers to handle the vulnerabilities of their products in compliance with the requirements of Annex II, Section 2. The regulation should instead demand that the manufacturer support a given product throughout its expected lifetime, whatever it might be: while a large part of consumer products have a lifespan shorter than five years, critical products for the enterprise market such as some operational assets in telecommunication networks are deployed for significantly longer and their lifetime is over ten years in many cases. This would mean that the manufacturers of those products would not be legally required to support them after the five-year deadline. For digital infrastructure to stay resilient, it is essential that the products used in the critical functions of networks remain supported during their whole lifetime, as stipulated in contracts between the manufacturer and the network operator. In B2B transactions, the manufacturer and its customer may want to agree on a specific lifespan for the product in the contract.

The expected product lifetime should be clearly defined and made available to prospective customers. The manufacturer should communicate for how long the product will be supported, as part of the technical documentation according to Article 23 and Annex V, and/or in the information and instructions rendered to the user as per Article 10(10) and Annex II. Where a vendor intends to make a change to the planned product EOL, sufficient prior notice should be mandated to allow the current product users to respond in a timely manner.

The treatment of legacy products that are already deployed and of products that are in a very advanced stage of development when the CRA enters into force needs to be clarified. This is particularly important for enterprise products with a long lifetime, such as telecommunication network equipment. These products should not be by default exempt from the regulation for their entire operational lifetime, to avoid gaps in the cybersecurity of critical connected environments even after the new CRA is in place. To cover this situation, the regulation should provide for a transition period during which manufacturers should gradually bring deployed products in compliance with the CRA requirements, following a risk assessment.

Reporting obligations

Article 11 requires that manufacturers notify to ENISA any actively exploited vulnerability of the product and any security incident "without undue delay and in any event within 24 hours of becoming aware of it". In many cases, the 24-hour delay for notifications would be far too short to allow the

manufacturer to establish the root cause and other important circumstances surrounding actively exploited vulnerabilities and security incidents. Achieving such awareness may require standard procedures and due diligence, over a longer period. Therefore, we recommend that the timing of the reporting obligations under the CRA align with the sensible procedure with staged deadlines put in place by the NIS 2 Directive – i.e., 24 hours for early warning; 72 hours for initial notification; 1 month for final report.

Considering the very wide scope of the CRA, the indiscriminate reporting of any security incident could put a strain on the sustainability and efficiency of the centralized notification system. The regulation should define what needs to be notified in order to really safeguard the resilience and security of digital products. Therefore, we recommend that manufacturers be compelled to only report significant incidents that have caused severe disruption of the digital product and has caused severe damage to the user and/or others, similar to what is required by the NIS 2 Directive.

The viability of the CRA reporting system does not only depend on realistic timescales and meaningful thresholds, but also and foremost on the efficient employment of public resources to operate the system. Therefore, we recommend that the CRA builds on the institutional setup introduced by the NIS 2 Directive: actively exploited vulnerabilities and security incidents should be communicated to the national CSIRT designated according to the directive, and to the national single point of contact in case of a large-scale attack. This partial decentralisation of the reporting system would make it more resource-efficient and would be all the more important for all those cases where an incident qualifies for reporting both under the CRA and the NIS2. A single notification could fulfil the reporting obligations under both laws, avoiding a duplicative administrative burden.

Finally, the CRA should ensure that the manufacturer of a critical product also informs legitimate business users of the actively exploited vulnerability or the security incident that has affected their product, as well as of any remedies that they should take, including available patches. Timely information on vulnerabilities and security breaches along the supply chain is vital for operators of critical infrastructure and essential services, like telecommunication providers, to ensure business continuity and asset resiliency. This information sharing should take place within the framework of the contractual relationship that binds the manufacturer and the business user.

Standards

The regulation should strongly promote the use of existing international standards, such as the standard for consumer IoT cyber security ‘ETSI EN 303 645’, and make it a condition that existing standards be leveraged wherever possible. Prescription of use of international standards allows customers to access the widest number of product options, lowers overall consumer costs through efficient product certification and compliance, engenders product confidence and enables effective market competition. Security standards should not be reinvented when fit-for-purpose existing standards already exist. If there are no international standards, then appropriate timescales should allow them to be developed in close cooperation with industry. Therefore, common specifications should only be used as a last resort and should be adopted based on robust governance principles and stakeholder participation.

Policy contacts:

Paolo Grassia
Director of Public Policy, ETNO
grassia@etno.eu

Lotte Abildgaard
Director Public Policy, GSMA
labildgaard@gsma.com