

EU Cyber Resilience Act

OVERVIEW

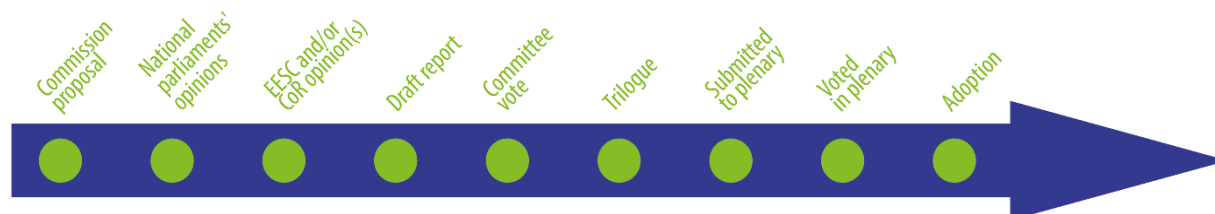
New technologies come with new risks, and the impact of cyber-attacks through digital products has increased dramatically in recent years. Consumers are increasingly falling victim to security flaws linked to digital products such as baby monitors, robo-vacuum cleaners, Wi-Fi routers and alarm systems. For businesses, the importance of ensuring that digital products in the supply chain are secure has become pivotal, considering three in five vendors have already lost money as a result of product security gaps.

The European Union's lawmakers signed the 'cyber-resilience act' in October 2024. The regulation imposes cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network. The regulation introduces cybersecurity by design and by default principles and imposes a duty of care for the lifecycle of products.

The Cyber Resilience Act was published in the EU's Official Journal on 20 November 2024. It entered into force in December 2024 and will apply in full as of 11 December 2027.

Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

<i>Committee responsible:</i>	Industry, Research and Energy (ITRE)	COM(2022)454 15.9.2022
<i>Rapporteur:</i>	Nicola Danti (Renew, Italy)	2022/0272(COD)
<i>Shadow rapporteurs:</i>	Henna Virkkunen (EPP, Finland) Beatrice Covassi (S&D, Italy) Ignazio Corrao (Greens/EFA, Italy) Evžen Tošenovský (ECR, Czechia) Matteo Gazzini (ID, Italy) Marc Botenga (The Left, Belgium)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
<i>Procedure completed:</i>	Regulation (EU) 2024/2847 OJ L, 2024/2847, 20.11.2024	



EPRS | European Parliamentary Research Service

Authors: Polona Car and Stefano De Luca
Members' Research Service
PE 739.259 – December 2024



Introduction

According to an industry [forecast](#), the total number of internet of things (IoT) connected devices worldwide is set to more than double from 13.2 billion in 2022 to 34.7 billion by 2028. Another [report](#) estimates that the number of devices connected to Internet Protocol (IP) networks will grow by 13 % by the end of 2024. Cybersecurity flaws in connected products come with a cost. In its 2020 report [Cybersecurity – Our Digital Anchor](#), the Commission highlighted how ransomware attacks hit organisations every 11 seconds around the globe. It is [expected](#) that by 2031 there will be a new attack on a consumer or business every 2 seconds, costing victims around US\$265 billion (€251 billion) annually. The European Union Agency for Cybersecurity's (ENISA) 2024 [report](#) on the threat landscape in the EU ranked cybersecurity threats such as Distributed Denial of Service (DDoS) and ransomware attacks at the top – accounting for over half of all observed incidents – with DDOS becoming increasingly large, complex and inexpensive, and increasingly targeting mobile networks and IoT.¹ In addition, the ENISA foresight report identified 'supply chain compromise of software dependencies' as the number one [cybersecurity threat](#) likely to emerge by 2030.

Given the growth in smart and connected products, a cybersecurity incident in one product can affect the entire supply chain, potentially disrupting social and economic activities across the internal market. An example is the [Kaseya VSA](#) supply chain attack of July 2021. This ransomware attacked over 1 000 companies and forced a supermarket chain to close all of its 500 shops across Sweden. Cisco [reports](#) that just 9 % of companies in Europe have a sufficiently mature level of readiness to be resilient against modern cyber threats.

In addition, European consumers' increasing use of connected devices (e.g. smart-home appliances) and the related risks should not be underestimated. According to a special Eurobarometer survey entitled 'The Digital Decade 2024', almost 80 % of EU citizens believed that improved cybersecurity, better protection of online data and safety of digital technologies would facilitate their use of digital technologies. Indeed, even toys have the potential to pose cybersecurity risks. In February 2017, the German regulator [banned](#) a connected doll, Cayla, which it deemed insecure both from a privacy point of view and as a potential concealed surveillance device. The doll could potentially allow anyone in close proximity to listen to and record conversations between the child and the toy by hacking the Bluetooth device connection.

Existing situation

In her 2021 [State of the Union](#) address, European Commission President Ursula von der Leyen announced the [cyber-resilience act proposal](#) (CRA). In recent years, there has been a substantial increase in the severity, intricacy and scale of cybersecurity threats, a trend also linked to escalation at the international level. To address the issue, the Council has [invited](#) the Commission to revise the EU's cybersecurity strategy. The importance of the cybersecurity topic was highlighted also in the [portfolio](#) of the Executive Vice-President for Tech Sovereignty, Security and Democracy.

The existing cybersecurity [strategy](#) already acknowledges that improving cybersecurity is essential for people to trust, use and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the right to protection of personal data and the freedom of expression. The existing EU cybersecurity framework comprises several pieces of legislation that cover specific aspects of cybersecurity from different angles.

The [Directive on Attacks against Information Systems](#), which focuses on criminal law, came into force in 2013 and harmonised criminalisation and penalties for a number of offences directed against information systems. A linked piece of legislation, the [Directive on Security of Network and Information Systems](#) across the EU (the NIS Directive) came into force in 2016, and introduced horizontal legal measures to boost the overall level of cybersecurity in the EU with a focus on protecting critical infrastructure. In December 2022, it was replaced by the [Directive on the Security of Network and Information Systems \(NIS2 Directive\)](#), which removed its predecessor's limitations and is to be transposed into national law by 17 October 2024. In addition, sectoral legislation, such

as the [Directive on the Resilience of Critical Entities \(CER\)](#) and the [Regulation on Operational Resilience of the Financial Sector \(DORA\)](#) set specific security and reporting requirements in their areas. As far as information and communication technology (ICT) products, services and processes are concerned, in 2019 the [EU Cybersecurity Act](#) strengthened the powers of ENISA and introduced a **voluntary certification scheme** to apply to the cybersecurity features of an ICT product, service or process. Although the scheme remains voluntary for businesses, it may be used for compliance with the mandatory safety requirements of other legal acts.

In addition, the EU has adopted specific sectoral legislation on safety for products with digital elements: the [Radio Equipment Directive \(RED\)](#), the [Medical Device Regulation](#), the [In Vitro Diagnostic Medical Devices Regulation](#), the [Vehicle General Safety Regulation](#), the [Common Rules in Civil Aviation Regulation](#) and the [Machinery Regulation](#). Lastly, the adopted [artificial intelligence act](#) mandates an ex-ante conformity assessment for [high-risk](#) artificial intelligence (AI) systems.² At present, there are no general cybersecurity requirements at EU level for any hardware and software that is not specific to certain products or sectors, as confirmed by Internal Market Commissioner Thierry Breton, who [said](#) that 'most of the hardware and software products are currently not covered by any legislation regarding their cybersecurity'. A 2019 [opinion](#) produced by the ENISA advisory group confirms this statement, reporting that 'connected devices for consumers often do not include the most basic security features, and are therefore vulnerable to the most basic cyberattacks and misuse'. In addition, the EU legal framework does not address the cybersecurity of [non-embedded software](#) represented by applications such as navigation software or in-car entertainment systems. Moreover, how economic operators address the vulnerabilities of products with digital elements throughout their lifecycle is an issue that demands further attention.

Member States have already adopted or proposed cybersecurity requirements for consumer IoT.³ However, the absence of a cybersecurity legal framework for products with digital elements incentivises the development of potentially diverging national rules among Member States, threatening the openness and competitiveness of the single market.

Parliament's starting position

In its 10 June 2021 [resolution](#) on the EU's cybersecurity strategy for the digital decade, Parliament called for security-by-design and cyber resilience for all internet connected products along the entire supply chain. Parliament welcomed the 'Commission's plans to propose horizontal legislation on cybersecurity requirements for connected products and associated services', with a view to harmonising national laws and hence preventing fragmentation of the single market. In addition, it asked the Commission to shape a horizontal regulation on cybersecurity requirements for apps, software (including embedded software), and operating systems by 2023. This regulation should require manufacturers to include information for users on the duration of security updates.

Council starting position

In its conclusions of [23 May 2022](#), the Council called on the Commission to propose, through the CRA, common EU cybersecurity requirements for connected devices and associated processes and services by the end of 2022. According to the Council, the proposal should take into account 'the need for a horizontal and holistic approach that covers the whole lifecycle of digital products, as well as existing regulation, especially in the area of cybersecurity'.

Preparation of the proposal

The European Commission outsourced a [study](#) to support the preparation of the [impact assessment \(IA\)](#) published together with the proposal. In addition, to collect stakeholders' opinions, the Commission held an [open public consultation](#) that closed in May 2022, and organised workshops, surveys and expert interviews. Special efforts were also made to gather SMEs' views on the impacts of the possible policy options. EPRS published an [initial appraisal of the Commission impact assessment](#) of the proposed cyber-resilience act in December 2022.

The changes the proposal would bring

As the first ever EU-wide legislation of its kind, the proposed [EU cyber resilience act](#) sought to bolster the cybersecurity of products with digital elements (digital products) in the European Union and to address existing regulatory cybersecurity gaps. Devices with digital elements that fail to meet the requirements of the CRA would be banned from the EU market. As the draft CRA was designed to also target digital products from non-EU vendors when marketed in the EU, it might have a potential impact on the cybersecurity standards for such products beyond EU borders. The EU would serve as the international point of reference on cybersecurity of connected devices the same way that the General Data Protection Regulation does for privacy. Indeed, rather than create different products or processes for different markets, non-EU companies might find it more convenient to apply the proposed mandatory CRA rules – and thereby secure an access to the EU single market for their digital products – as a default framework for their global operations.

Principle and objectives

The proposed CRA was a **piece of horizontal legislation** based on Article [114](#) of the Treaty on the Functioning of the EU (ordinary legislative procedure applies) dealing with legislative harmonisation and the establishment and functioning of the internal market. It aimed to harmonise cybersecurity rules for the placing on the market of products with digital elements. EU standards based on the CRA would raise the level of cybersecurity for digital products, benefiting both businesses and consumers.

The proposed CRA had two main objectives for digital products (i.e. hardware and software), and its aim was to create the conditions for the development of secure digital products, by ensuring that hardware and software products are placed on the market with fewer vulnerabilities. It also aimed to oblige manufacturers to take security seriously throughout products' lifecycles, and to encourage users to take cybersecurity into account when selecting and using products.

Scope

In Article 3(1), the proposed CRA defined **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'. In Article 2(1), it further clarified that the proposed regulation applies to 'products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network'. Therefore, the proposed CRA was a horizontal regulation that, with a few exceptions, covered a very wide range of digital products, such as connected devices (e.g. consumer and industrial IoT), operating systems and non-embedded software. The proposal also covered AI systems, including the cybersecurity of products with digital elements that are classified as high-risk AI systems.

Excluded from the proposal's coverage were digital devices covered by specific sectoral regulations⁴ and software-as-a-service ([SaaS](#)), such as clouds, unless they were part of integral remote data processing solutions for a product with digital elements. Last but not least, in order not to hamper innovation or research, free not-for-profit open source software was not covered by the proposal.

The proposed CRA divided the digital products it covers into two main categories, based on their level of risk. The first is **default non-critical products**, i.e. hardware and software with a low level of criticality (e.g. hard drives, smart home assistants or connected toys). The second is **critical products** (listed under Annex III), which are further divided into [two sub-categories](#), class I lower risk (e.g. virtual private networks and routers) and class II higher risk (e.g. operating systems for desktops and mobile phones or smart meters) reflecting criticality and intended use.

Based on their level of risk, the above-mentioned digital products would be subject to less or more stringent conformity assessment procedures to demonstrate compliance with the cybersecurity obligations set in the proposed regulation. Such procedures range from a simple cybersecurity self-assessment to a third-party conformity assessment.

For **non-critical products**, which represent 90 % of digital products placed on the market, manufacturers would have to declare under their own responsibility that the devices with digital elements comply with all the security requirements defined in the draft CRA (self-assessment).

For **critical products**, the process to demonstrate compliance differs, based on the sub-category taken into consideration. For **critical class I** products (lower risks), the manufacturer may still carry out a self-assessment under their own responsibility as long as they apply to their product existing i) harmonised cybersecurity standards (e.g. developed by European standardisation organisations); or ii) cybersecurity certification schemes under the EU Cybersecurity Act. In the absence of such standards and schemes for the product in question, or if the manufacturer has not applied or has only applied in part the standards or schemes, the manufacturer would have to undertake a conformity assessment

performed by a third party (conformity assessment body, CAB). For **critical class II** products, manufacturers would be subject to the third party conformity assessment run by a CAB.

The proposed CRA placed cybersecurity obligations on different economic operators in accordance with their roles and responsibilities in the supply chain. **Manufacturers** would need to ensure that digital products comply with essential cybersecurity requirements and conformity assessment procedures before placing them on the market. In addition, they would need to record technical documentation and abide by notification obligations for cybersecurity breaches. **Importers** would have to place on the market only digital products that comply with essential cybersecurity requirements and bear the CE marking. **Distributors** would have to verify that the digital products bear the CE marking. They would also have a duty of care to ensure that manufacturers and importers have complied with their obligations under the act.

Main provisions

Cybersecurity by design and by default

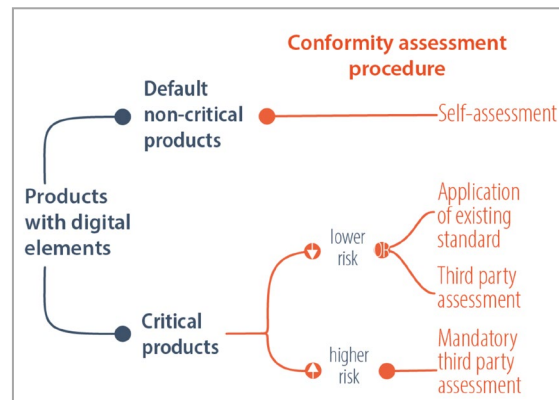
Manufacturers would be required to consider cybersecurity starting from the design and development phase of the digital product, by using secure-by-default configurations and avoiding known exploitable vulnerabilities. The annexes of the proposed CRA include: i) the information manufacturers should make available to users; ii) conformity assessment procedures digital products would have to go through; and iii) the technical documentation that needs to be provided. In addition, Annex I (2) details the vulnerability handling requirements manufacturers would have to follow to assure the cybersecurity of digital products.

Essential cybersecurity and vulnerability handling requirements, including reporting obligations

The proposed CRA split the cybersecurity obligations for manufacturers into i) security requirements relating to the properties of digital products; and ii) vulnerability handling requirements.

Significant **cybersecurity requirements** listed in Annex I include obligations to: i) design, develop and produce digital products in such a way that limits their attack surface and reduces the impact of any incident based on the risks; ii) deliver digital products without known exploitable vulnerabilities; iii) protect the confidentiality and integrity of data stored, transmitted or processed; iv) process only data, personal or other, that are strictly necessary to the functioning of the digital product – 'data minimisation'.

Figure 1 – Cyber-resilience conformity assessment



Source: European Commission.

As regards **vulnerability handling**, after the product has been placed on the market, manufacturers would have to deploy, among other things, regular tests and reviews of their digital products' security, keep a record of vulnerabilities identified, and remediate them by providing free security updates and patches. The manufacturers will be required to do so for the expected product lifetime or for a period of five years, whichever is shorter.

Finally, manufacturers will have to report actively exploited vulnerabilities and security incidents to ENISA within 24 hours of becoming aware of them.

Conformity assessment and compliance

The type of conformity assessment procedure applied to demonstrate compliance with the requirements mentioned above depends on the criticality of the digital product (see Figure 1). The digital products demonstrating compliance with the security requirements and the conformity assessment procedures will obtain an EU declaration of conformity valid in all EU Member States and will bear the CE marking according to the general principles of Regulation (EC) 765/2008.

Fines

Member States will appoint market surveillance authorities, which will be responsible for the enforcement of the proposed CRA obligations. In case of non-compliance with the obligations set out in the proposal, the following maximum fines would apply depending on the type of infringement and nature of the economic operator. **Manufacturers**, for instance, could risk a fine of €15 million or 2.5 % of their total annual turnover worldwide, whichever is higher, for non-compliance with the security requirements listed under Annex I. **Manufacturers, importers, or distributors** could risk a fine of €10 million or 2 % of their total annual turnover worldwide, whichever is higher, for non-compliance with any other obligation laid down in the draft regulation.

Interplay between the conformity assessment procedure and existing or upcoming cybersecurity legislation

The proposed CRA and the conformity assessment procedure it lays out dovetail with other pieces of existing or proposed legislation on cybersecurity. The proposal aimed to harmonise the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements without overlapping with requirements stemming from the pieces of legislation listed below.

Starting with **existing legislation**, the CRA proposal would complement the baseline EU cybersecurity framework, namely the NIS2 Directive and the EU Cybersecurity Act. The NIS2 Directive puts in place cybersecurity requirements and incident reporting obligations for essential and important entities with a view to increasing their resilience – for example, a clear obligation to demonstrate how those entities have assessed the security level of the ICT products and services. Therefore, the enhanced and certified level of cybersecurity of products with digital elements – to be reached through the CRA – would facilitate compliance by the entities within the scope of the NIS2 Directive and strengthen the security of the entire supply chain.

The EU Cybersecurity Act provides for the development of voluntary certification schemes. Each scheme includes references to relevant standards, technical specifications and other cybersecurity requirements defined in the scheme. Digital products respecting such voluntary cybersecurity certification schemes would be presumed to be compliant with the conformity assessment provided for in the proposed CRA. Finally, the proposed CRA applies to radio equipment within the scope of the RED delegated regulation. The proposal is aligned with those requirements of the RED delegated regulation that impose high-level standards on manufacturers of internet-connected wireless and wearable radio equipment. To avoid a regulatory overlap, the Commission would repeal the RED delegated regulation with respect to specific radio equipment that is also covered by the proposed CRA once it enters into force.

Digital products covered in the Machinery Regulation, and for which a conformity assessment is required, would be considered to be in conformity with the proposed CRA, providing the health and safety requirements of the sectoral Machinery Regulation are met.

As regards **legislative proposals** under adoption, the conformity assessment procedure under the proposed CRA would also take into consideration the provisions of the artificial intelligence act. As a general rule, for devices also classified as high-risk AI systems, the conformity assessment procedure under the proposed CRA would serve to demonstrate compliance with the security requirements under the artificial intelligence act. However, exceptions apply to certain AI critical products.

Advisory committees

The [European Economic and Social Committee](#) (EESC) adopted its [opinion](#) during its plenary session of 14-15 December 2022.

National parliaments

The subsidiarity deadline for national parliament was [19 December 2022](#). Only the [Czech Chamber of Deputies](#) has issued a reasoned opinion.

Stakeholder views⁵

Scope of the proposal: What kind of software?

According to [DigitalEurope](#), representing the digital technology industry in Europe, the inclusion of all software within the scope of the proposal would have been an excessive and premature step, as cyber-resources are scarce both for the industry and for governments. On the other hand, [Eurosmart](#), representing the European digital security industry, supported the inclusion of software as a product under the relative liability rules, as this would help to acknowledge the cybersecurity value chain when products relying on software are placed on the market. [Internet Society](#), a non-governmental organisation (NGO) promoting internet development, pleaded for clear exclusion of not-for-profit open-source licence software from the scope of the CRA, because of the unclear definition of commercial activity in the proposal. [Business Europe](#), representing enterprises of all sizes, also deemed it necessary to have additional clarification regarding the exclusion of open-source software that is not used in the course of a commercial activity. [Industry coalitions repeatedly](#) urged the co-legislators to exclude not-for-profit open-source software from the scope of the CRA.

Personal data as essential cybersecurity requirements

The [European Data Protection Supervisor](#) (EDPS) recommended considering personal data protection to be an 'essential cybersecurity requirement' for products with digital elements. This should have been done by applying the principle of data protection by design and by default. The proposal should have clarified that it does not aim to affect the powers of data protection authorities.

Classification of products based on risk

[APPLiA](#), representing the European home appliance industry, advocated making a clear distinction between low and high-risk products and defining clear standards for each of the two categories. The [European Digital SME Alliance](#) called for a risk-based approach, where different product categories would follow different procedures (e.g. imposing minimum requirements and compliance checks for low-risk products). [Euroconsumers](#), association of consumer organisations, believed that the omission of consumer IoT products (e.g. connected devices intended for children) from the category of critical products should have been reconsidered. Such products could be potentially harmful if hacked, and a third-party risk assessment could play a role in detecting vulnerabilities in them. [BEUC](#), the European Consumer Organisation, confirmed this position and stated that the CRA should have introduced a European cybersecurity certification scheme for all critical products as an alternative to proving their conformity. [TIC Council](#), representing the testing, inspection and certification industry, was similarly concerned about the nature of consumer IoT products that currently fall within the low-risk category despite having the ability to collect, store and share data. [Developers Alliance](#) stressed that the Commission retains a large margin of discretion for updating

the list of critical products under Annex III. [Eurosmart](#) urged for precise category definitions for products included in Annex III. Similarly, an [industry coalition](#) advocated for a proportionate approach to determining product risk levels in order to avoid unjust designation of too many products as critical.

[VDMA](#), representing the mechanical and plant engineering industry, was concerned that classifying all core components for networked machines and systems as critical products could have led to red tape for manufacturers. According to them, many industrial components are only used for non-critical purposes. They feared that this approach could cause delays in the deployment of digital products and their components in Europe, and proposed making a reference to the intended use of the products. The [CEOs of six European techs companies and Digital Europe](#) warned that a wide scope of CRA could create COVID-19 style disruptions in the EU supply chains because of bottlenecks created by obliging manufacturers to certify their products through third-party certifiers. Therefore the number of higher risk products in Annex III should be minimal. Similarly, an [industry coalition](#) believed that most products from Annex III should be placed into the non-critical category and should consequently adhere to self-assessment, to avoid excessive costs for launching new products.

Conformity assessment procedure

[BEUC](#) argued in favour of independent third-party conformity assessments also for certain products representing higher risks to consumers (e.g. safe home systems). In a similar vein, the [TIC Council](#) favoured conformity assessment by bodies that are independent from the product developer. They were afraid that, as 90 % of the digital products subject to the proposed CRA will still be assessed by their manufacturers, this would leave on the market a certain amount of products that can pose risks to consumers' safety and security. Furthermore, the TIC Council [demanded](#) that the TIC industry be fully recognised as a trusted partner in cybersecurity conformity assessments. [TÜV Verband](#), association of technical inspection agencies, believed that the CRA should 'not only define cybersecurity requirements, but it must also stipulate effective instruments with which compliance with these requirements can be reliably verified'. The association considered that all critical products should undergo a compulsory assessment by independent assessment bodies. In contrast, the [CCIA](#), computer and communications industry association, considered the conformity assessment procedures for digital products to be excessive, with the potential to stop the development of new technologies and services.

Concerns were expressed over the absence of horizontal cybersecurity standardisation schemes. For example, [VDMA](#) worried that the absence of appropriate standards could cause delays in the delivery of approved products. [Eurosmart](#) encouraged different standardisation initiatives to support certification schemes for different product types as described by the CRA. They believed that the cybersecurity of critical products with digital elements should be assessed under the EU Cybersecurity Act's certification scheme at its 'high' level. Applying this scheme to critical products with digital elements would provide a presumption of conformity with the CRA requirements, because it contains mandatory penetration testing – the only way to seriously assess the robustness of such products. They also [recommended](#) making use of all available European standards rather than using only '[harmonised standards](#)', which would have a limiting effect.

Duty of care and product lifecycle

[Euroconsumers](#) had reservations about the definition of the expected product lifetime, where the duty of care (the duty on manufacturers to monitor and address any vulnerabilities for the 'expected product lifetime') was set at a maximum of five years. This could be problematic, for example, for users of smart home security systems that are expected to last much longer than five years. Along these lines, [BEUC](#) asked for including a requirement that manufacturers provide software updates for the whole lifecycle of a product and differentiate between [functionality and security updates](#). Contrary to this, the [European Digital SME Alliance](#) welcomed the time limit for of the duty to provide updates. An [industry coalition](#) rejected the differentiation between security and

functionality updates as 'not feasible'. They believed that linking expected product lifetime solely to reasonable user expectations creates legal uncertainty. [Eurosmart](#) advocated that manufacturers should be free to define a product's expected lifetime based on its technical capacities, but they should clearly indicate it in a declaration of conformity.

Notification fatigue, reporting of unpatched vulnerabilities and transitional period

[Blackberry](#) drew attention to the burden on companies to report cybersecurity incidents to different authorities. [BEUC](#) believed that ENISA should be the central reporting entity to which any incident needs to be reported. The American Chamber of Commerce to the European Union ([AmChamEU](#)) suggested aligning the CRA's obligations on notifications with existing or draft legislation covering cyber incidents (e.g. the NIS2 Directive). Similarly, a [group of CEOs](#) supported the idea to extend the approach of the NIS2 Directive, where only significant risks are reported and the 'one incident-one report' principle applies. [Eurosmart](#) welcomed the proposal for manufacturers to report only significant incidents, which however should be clearly defined.

European Digital Rights (EDRI), an association of digital civil and human rights organisations, [called](#) for the inclusion of safeguards in addressing the vulnerability disclosure requirements to avoid the misuse of information related to vulnerabilities. Similarly, a [coalition](#) of national, European and international associations urged for the removal of the obligation on the reporting of unpatched vulnerabilities and for limiting it only to disclosure of vulnerabilities where mitigation actions are available. This echoes the position of the [digital industry coalition](#). It was furthermore reiterated in an [open letter](#) drafted by 57 cybersecurity experts, and in the position of another [industry coalition](#). If actively exploited vulnerabilities remain in the scope of the regulation, a [group of CEOs](#) asked for the manufacturers to decide, at their discretion, between patching the vulnerability or immediately reporting it.

[Orgalim](#), representing Europe's technology industries, asked that a transition period of 48 months after the entry into force of the CRA be given to ensure that the industry is prepared to comply with the new provisions. Various industry coalitions have demanded similar transition periods, ranging from [48](#) to [72 months](#). The [TIC Council](#), on the other hand, rejected the postponement of the implementation deadline.

Academic views

Need for horizontal regulation

Ludvigsen and Nagaraja⁶ recommended applying the proposed regulation to the entire supply chain and support the full transparency concept. This means that understanding the cryptography and cybersecurity tools of the product would not qualify as a trade secret for the purposes of non-disclosure of information (except for certain exemptions such as hardware verification mechanisms). Similarly, Chiara⁷ advocated harmonised EU cybersecurity rules, as this would be the most efficient way to increase cyber resilience by enhancing the trust of users and the prominence of products with the CE marking. According to the author, the CRA contributes to the evolution of the concept of cybersecurity and goes beyond technical IT security. A horizontal approach would help to ensure legal certainty by avoiding further overlapping of legislation and market fragmentation. In addition, Chiara believed⁸ that such an approach underpins the cybersecurity principle enshrined in the [European Declaration on Digital Rights and Principles](#) and would be fit to enforce it. Burri and Zielhmann⁹ warned that the overarching goal of the CRA to be the global cybersecurity standard-setter could have the adverse effect – that of causing the fragmentation of the global data governance. The [Center for Data Innovation](#), meanwhile, stated that the horizontal framework under the CRA could entail high compliance costs and might not be sufficiently future-proof. Therefore, they recommended a sectoral approach to cybersecurity regulations, which would also minimise costs.

Risk-based approach and continuous risk assessment

According to the Center for Data Innovation's above article, the CRA should have included a requirement for continuous security risk management, where digital products should be kept secure throughout their lifecycles, with penetration testing being part of this maintenance system. The authors advocated that it should be the Member States' dedicated authorities and not private organisations that should be assessing the security of digital products. Burri and Zielhmann questioned the appropriate level of cybersecurity and protection, given that 90 % of digital products will undergo self-assessment by manufacturers. They questioned as well the decision to exclude from the set of considerations the environment in which a certain product will be placed, as threats and risks depend greatly on it. In addition, setting the expected lifetime of products to five years might create flaws, considering that many products have a longer lifetime or have already been on the market for some time, possibly beyond the expiration of the five-year deadline.

Surveillance and enforcement

Ludvigsen and Nagaraja also made several interesting proposals regarding surveillance and enforcement. Their article outlined two possible approaches for the CRA: creation of common rules at EU level and their enforcement at national level; or harmonising some measures at EU level through a central authority, such as ENISA, and entrusting the remaining ones to the national authorities. Both approaches will need to take into account the voluntary certification schemes that have been provided for by the Cybersecurity Act. Finally, the authors recommended adopting stringent enforcement mechanisms by giving national authorities inspection powers. As far as staff and sanctions are concerned, they suggested staffing requirements similar to those in the AI act proposal and sanctions similar to those envisaged in the GDPR, with the additional possibility of banning cyber insecure products from the market.

Burri and Zielhmann found that the criteria for market surveillance authorities to intervene in specific cases are too broad and too vague. In addition, they highlighted the potential coordination problems among different national authorities because of complexity of monitoring and oversight. They warned against the risk of fragmentation of surveillance and consequently imbalance between national market surveillance authorities inside the EU because of unclear wording of the proposal, which gives the market surveillance authorities the discretion to investigate products or not to do so. More attention should also be paid to the relationship between the imposition of fines and the banning of products from the EU market, which is not yet clear enough.

Legislative process

In the Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE), with Nicola Danti (Renew, Italy) as rapporteur. The Committee on Internal Market and Consumer Protection (IMCO) had exclusive competence on Articles 7 and 9 and shared competence on Articles 4, 8, 21, 22 and 25-40 of the proposal. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) had shared competence on Article 41(5) of the proposal. Both the IMCO and LIBE committees had been asked to submit opinions. [IMCO](#) published its opinion on 30 June 2023, whereas the LIBE committee decided not to give an opinion.

The ITRE committee adopted its [report](#) on 19 July 2023. The main points of the committee amendments to the Commission proposal include:

- **Scope:** The report confirmed the Commission's proposal to include all products with digital elements. It underlined however the need to ensure that developers of open-source software are excluded from the scope if they are not receiving any financial returns for their projects. The report expanded the list of critical products under class I, to also include home automation systems and products that enhance private security, such as cameras and smart locks.
- **Expected product lifetime:** The report gave manufacturers flexibility to determine the length of the period over which they would ensure that vulnerabilities are handled; greater clarity is needed in this regard. Manufacturers would be obliged to provide automatic security updates,

with an easy-to-use option for deactivation for the users. Where feasible, they would also need to differentiate between security and functionality updates. When the support period is shorter than five years, the manufacturers would need to make their source code available to companies that want to provide security updates.

- **Reporting** would need to align with the NIS2 Directive in order to simplify the obligations for manufacturers, and make mandatory only reporting of significant incidents and actively exploited vulnerabilities, done through a multi-step approach (24 hours, 72 hours, one month). ENISA would become the one-stop entity for reporting. It should receive reinforcement to be able to fulfil its additional tasks under the regulation.
- **Application deadline:** The report proposed to prolong the moment from which the regulation applies to 36 months. In this respect, micro, small and medium-sized enterprises need to receive sufficient support to ensure their compliance. Harmonised standards and common specifications or European cybersecurity certification schemes need to be in place six months before the conformity assessment procedure starts applying. The Commission would need to provide guidelines with more details on the implementation.
- **Cybersecurity workforce.** The report underlined the importance of cybersecurity professionals and proposes up-skilling and re-skilling to ensure their availability.
- **Mutual recognition agreements (MRAs)** with third countries are proposed to promote international trade and ensure the same level of protection as that provided by the CRA. As regards the monitoring of non-technical risk factors, ENISA and market surveillance authorities would need to perform the necessary checks on vendors that might present a higher risk.

In the Council, Coreper also [reached](#) a common position on 19 July 2023, allowing the Council to enter into negotiations with the Parliament. Council notably removed the notion of 'critical' from products with digital elements and deleted a substantial number of the products listed in Annex III. Council introduced three categories of products – hardware devices with security boxes, smart meters and smart cards, grouped in a new Annex IIIa. These products, which are critical for the essential entities as defined by the NIS2 Directive, would fall under mandatory European cybersecurity certification schemes. The products' lifetime would be determined by the manufacturers, who would need to specify the year and month until when they will handle vulnerabilities. The Council moved the reporting of cybersecurity incidents and actively exploitable vulnerabilities from ENISA to the national Computer Security Incident Response Teams (CSIRTs) in a two-step process of an initial notification after 24 hours and a second one after 72 hours. Council proposed to postpone the application of the regulation to 36 months as also envisaged by the Parliament.

Parliament confirmed the decision of the ITRE committee to enter into interinstitutional negotiations on [13 September 2023](#). The co-legislators met in trilogue negotiations on 27 September and 8 November 2023, and reached a provisional agreement on the text during the third trilogue on 30 November 2023.

The agreed text simplifies the methodology for the classification of digital products. MEPs secured an expansion of the list of covered devices with products such as identity management systems software, password managers, biometric readers, smart home assistants and private security cameras. The support period for manufacturers shall be at least five years, with the differentiation between security (automatically installed) and functionality updates. For reporting, initial recipients will be competent national authorities, who will notify ENISA to be able to assess the situation and, if they estimate that the risk is systemic, inform other Member States so they are able to take the necessary steps.

Application of the regulation is postponed for 3 years after its entry into force to give manufacturers sufficient time to adapt. The negotiators also agreed to add to the text support measures for small and micro enterprises, including specific awareness-raising, education and training programmes, collaboration initiatives, and strategies to enhance workforce mobility, as well as support for testing and conformity assessment procedures.

In the Council, Coreper confirmed the agreement in December 2023. The ITRE committee approved the provisional agreement in January 2024; Parliament [adopted](#) the text in March 2024 and approved a [corrigendum](#) in September 2024. The Council approved the text in October 2024. The Cyber Resilience Act was formally signed on 23 October 2024 and published in the Official Journal on 20 November 2024.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Negreiro, M., [The NIS2: A high common level of cybersecurity in the EU](#), EPRS, European Parliament, February 2023.

Negreiro, M., [ENISA and a new cybersecurity act](#), EPRS, European Parliament, July 2019.

Vikolainen, V., [Strengthening cyber resilience](#), EPRS, European Parliament, December 2022.

OTHER SOURCES

European Parliament, [Horizontal cybersecurity requirements for products with digital elements \(Cyber Resilience Act\)](#), Legislative Observatory (OEIL).

Joint Research Centre, [Cybersecurity, our digital anchor](#), European Commission, 2020.

ENDNOTES

- ¹ Internet of things (IoT) devices and networks are increasingly suffering from DDoS attacks as their resources are often limited, which causes poor security features. Weak passwords, for example, make devices easy to corrupt.
- ² See definition in Article 6 AI act.
- ³ For example, [Finland](#) and [Germany](#) apply certain security measures on a voluntary basis. Non-EU countries are also busy addressing this issue; for example, [Brazil](#), [China](#) and [Japan](#) have adopted mandatory certification schemes for certain digital products. In the UK, a [law](#) has introduced mandatory security requirements and required a statement of compliance before a consumer IoT product can be placed on the market. In the US, an [Executive Order on Improving the Nation's Cybersecurity](#) has been published, identifying software bills of materials (SBOMs) as a crucial tool to improve the security and integrity of the software supply chain (see Congressional Research Service [report](#)).
- ⁴ Regulations on medical devices, in-vitro diagnostic medical devices, civil aviation safety, on-type approval requirements for motor vehicles and their trailers and systems. Furthermore, components and products developed exclusively for national security or military purposes and products specifically designed to process classified information are also excluded from the scope of the proposed CRA.
- ⁵ This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.
- ⁶ See K. Ludvigsen and S. Nagaraja, [The Opportunity to Regulate Cybersecurity in the EU \(and the World\): Recommendations for the Cybersecurity Resilience Act](#), Cornell University, May 2022.
- ⁷ See P. Chiara, [The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements](#), International Cybersecurity Law Review, November 2022.
- ⁸ See P. Chiara, [Towards a Right to Cybersecurity in EU Law? The Challenges Ahead](#), August, 2023.
- ⁹ See M. Burri and Z. Zihlmann, [The EU Cyber Resilience Act – An Appraisal and Contextualization](#), *Zeitschrift für Europarecht* (EuZ), 2/2023, B1-B45, February 2023.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2024.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

<http://epthinktank.eu> (blog)

Fourth edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.