BDI

POSITION | DIGITALISATION | CYBERSECURITY

Cyber Resilience Act

Introducing cybersecurity requirements for products with digital elements

1 December 2022

Executive Summary: Increasing the cyber-resilience of products with digital elements

Companies, operators of critical infrastructures and private users are experiencing a steady increase in cyber-attacks. Often, cybercriminals are exploiting vulnerabilities in products with digital elements. While the attackers only have to know one of these technological weaknesses to cause significant harm, manufacturers and operators have to protect all their products and systems against an ever-increasing threat landscape. Therefore, German industry advocates for the implementation of risk-adequate cybersecurity measures across all products with digital elements during the design, development and production phases as well as when and while a product is placed on the market. We therefore support the European Commission's proposal for the Cyber Resilience Act (CRA) in principle. The Cyber Resilience Act will – unlike the Cybersecurity Act – horizontally introduce cybersecurity requirements across product categories based on the principles of the New Legislative Framework. Moreover, the essential cybersecurity requirements introduced by the CRA will help essential and important entities to fulfil the supply-chain-related cybersecurity requirements introduced by Article 19 of the NIS 2-Directive. The interplay between CRA and NIS 2 will contribute to security in operations and configuration of critical infrastructures and other companies where secure products are just one, albeit important, factor for a risk-adequate level of cyber resilience.

Improving the Commission's proposal

While German industries appreciate the Commission's proposal in general, we nonetheless see some areas, where the proposal should be improved during the upcoming legislative process. We would appreciate if the European Parliament and the European Council would take into account the following proposals:

- **reporting obligations:** As determining the impact of known vulnerabilities as well as evaluating safety and appropriateness of available mitigations will require considerable resources, we urge the European co-legislators to increase the reporting period to 72 hours and mirror the reporting infrastructures which have been established under NIS 2.
- **Scope:** While we support the Commission's intention to include a scope that is as broad as possible, the text creates confusion, for example, as to what type of "software" should be covered by the new rules, and what is precisely meant with software with "remote data

Steven Heckler | Digitalisation and Innovation | T: +49 30 2028-1523 | s.heckler@bdi.eu | www.bdi.eu

processing". We specifically support a clearer exclusion of SaaS from the scope of the proposed CRA as SaaS is a service, not a product, and is already covered by the requirements under the NIS 2 Directive (as cloud services, including SaaS, are listed as "essential services"). Moreover, with respect to free and open-source software, it remains unclear whether it is in the Cyber Resilience Act's scope or not.

- **terminology:** In order to better express intentions, the term "known exploitable vulnerability" should be substituted by "exploitable vulnerability known to the manufacturer". This is important, since secret services and other public bodies of the EU Member States are frequently aware of vulnerabilities, i.e. "known exploitable vulnerabilities", of which they do not inform the manufacturer. As manufacturers can only mitigate vulnerabilities of which they are aware / made aware, EU Member States should be obliged to share their knowledge of vulnerabilities with the respective manufacturers of products with digital elements and on relevant notification platforms – notably established CERT services.
- **critical products with digital elements:** In its proposal, the European Commission differentiates between four types of products with digital elements: products with digital elements, two classes of critical products with digital elements, and highly critical products with digital elements. German industry appreciates this approach in principle as such a differentiation follows the necessary risk-based approach. However, German industry considers the two classes of products with digital elements to be defined as "critical", which include, for example, microcontrollers, industrial automation and control systems or parts of the Industrial Internet of Things, as too broad. Rather than addressing product groups in general, the EU co-legislators should consider the intended use of products with digital elements and their specific criticality, as one and the same product can perform a more or less critical function according to the concrete application scenario.
- **implementation:** The Cyber Resilience Act's very broad scope has far-reaching implications for its implementation. At the same time, the CRA will only become fully effective once the organisational framework conditions specified in the law are in place. German industry believes that the implementation period of 12 to 24 months is too short to implement the essential requirements across all products with digital elements according to Article 2 (1). This is the case, as the Cyber Resilience Act constitutes the first regulatory act on the European internal market to horizontally regulate the cyber resilience of products. Consequently, companies across sectors have to review their internal measures for CRA-conformity / or even have to set up respective measures, and have to implement a vulnerability handling mechanism that accommodates the requirements set out in Annex I Section 2. Moreover, the Member States must organise the market surveillance outlined in Article 43. To this end, new organisational structures have to be defined and new employees have to be hired. Furthermore, harmonised European standards have to be developed – either from scratch or based on IEC 62443. To this end, the European Commission has to issue the standardisation request. All this will take more than the proposed 12 to 24 months. Henceforth, we urge the European Commission to prolong the implementation period to 36 months.
- **labelling:** The European co-legislators should avoid the introduction of any kind of additional cybersecurity protection / risk product labels. In any case, if a Member State or the European Commission were to introduce such a label, it should not be static as the cybersecurity risk is constantly evolving.

Table of content

Rationale for a horizontal cybersecurity regulation for products with digital elements based on the principles of the New Legislative Framework

The increasing spread of digital technologies is creating a wide range of new opportunities – for both private and commercial users. At the same time, digitalisation also poses numerous challenges in terms of security and privacy, which can lead to additional risks. These risks can be mitigated by employing targeted technical, regulatory, and behavioural measures (such as security-by-design) in development processes as well as during configuration and operations.

A high degree of cyber resilience is a basic prerequisite for the trouble-free functioning of highly digitalised processes, connected products and services. Moreover, in light of recent political developments (e.g. the Russian war against Ukraine, tensions with China as well as the surge in state-sponsored cyberattacks), strong European cyber resilience is essential for the protection of our democracy, free societies and security. Coherent legal provisions are key to maintaining the international competitiveness of German and European industry. It is important to consider that products – understood as hardware, software and combinations thereof – are integrated into highly complex systems, which means that, when regulating them, these interactions must also be accommodated.

The European and national legislators are currently developing a very broad regulatory cybersecurity framework. Following the introduction of technical and organisational requirements to enhance the cyber resilience of essential and important entities, the European Commission's proposal for a Cyber Resilience Act now addresses the cyber resilience of all products with digital elements and their components. In contrast to product-specific cybersecurity certification schemes pursuant to Regulation 2019/881, such as the EU Cloud Scheme (EUCS) and the likely upcoming EU 5G Scheme (EU5G), the Cyber Resilience Act – by covering a very broad scope of products – functions as a horizontal regulation and thereby helps to avoid a regulatory hotch-potch. Such a hotch-potch of regulatory initiatives would run the risk of introducing diverging requirements and would likely omit certain product groups. Therefore, German industry supports the approach taken by the European Commission to propose a horizontal cybersecurity legislative act based on the principles of the New Legislative Framework (NLF) that introduces mandatory essential cybersecurity requirements and a vulnerability handling mechanism for manufacturers. Such a horizontal approach is preferable to introducing cybersecurity requirements in different product-specific legal acts. In this regard, German industry would appreciate if the ENISA and the European Commission were to limit the development of cybersecurity certification schemes under the Cyber Security Act to the absolute necessary minimum.

In detail discussion of selected articles from the EU Commission's proposal for a Cyber Resilience Act

Ensuring a risk-adequate degree of cyber-resilience across the European Union is of outstanding importance in light of the increasing interlinkages between sectors, actors and along supply-chains. Therefore, German industry appreciates that the European Commission issued a proposal for a regulation that introduces essential cybersecurity requirements that products with digital elements as well as their manufacturers in terms of vulnerability handling have to fulfil. Nonetheless, we perceive the need that the European Council and the European Parliament alter the Commission's proposal in such a way as to take into account the requirements of German industry – both as producers as well as users of products with digital elements.

Subject matter (Article 1)

German industries appreciate the European Commission's holistic proposal that addresses the various stages during the lifecycle of a product with digital elements in terms of rules for the placing on the market, the product's cybersecurity characteristics, the manufacturer's vulnerability handling processes, as well as the market surveillance and enforcement processes. Thereby, the Cyber Resilience Act will contribute to a significant increase in the European Union's cyber-resilience. At the same time, the Cyber Resilience Act's broad scope poses significant challenges in terms of implementations. For example, manufacturers of products with digital elements face vast problems when attempting to recruit cybersecurity experts, as Germany alone currently has a cybersecurity workforce gap amounting to more than 104,000 cybersecurity experts[1]. Similarly, market surveillance bodies across the EU face huge challenges in getting the talent required for cybersecurity-related market surveillance activities, especially since such public bodies are confronted with a structural deficit in terms of lower salaries. Moreover, the implementation of the CRA requires far-reaching activities by European standardisation organisations, which also will require time. Henceforth, the European co-legislators should prolong the implementation period to 36 months.

Scope (Article 2)

German industry welcomes the European Commission's proposed scope which includes all "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". German industry very much appreciates this horizontal approach because Europe's cyber-resilience will only increase if all products with digital elements comply with risk-based cybersecurity requirements according to their intended use. However, this very broad scope has far-reaching implications for the implementation of the Cyber Resilience Act. German industry believes that the implementation period of 12 to 24 months is too short to implement the essential requirements across all products with digital elements according to Article 2 (1). This is the case, as the Cyber Resilience Act constitutes the first regulatory act on the European internal market to horizontally regulate the cyber resilience of products. Consequently, companies across sectors have to review their internal measures for CRA-conformity / or even have to set up respective measures, and have to implement a vulnerability handling mechanism that accommodates the requirements set out in Annex I Section 2. Moreover, the Member States have to organise the market surveillance outlined in Article 43. To this end, new organisational structures have to be defined and new employees have to be hired. Furthermore, harmonised European standards have to be developed – either from scratch or based on IEC 62443. To this end, the European Commission has to issue the standardisation request. Afterwards, manufacturers of products with digital elements have to consider respective requirements in the design and development of products. All this will take more than the proposed 12 to 24 months. Henceforth, we urge the European Commission to prolong the implementation period to 36 months.

Additionally, SaaS should be more clearly excluded from the scope of the proposed CRA. Recital 9 specifies that the proposed CRA does not regulate SaaS except "for remote data processing solutions". However, 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". This lacks the necessary clarity for software developers. Under NIS 2, cloud services (which also include SaaS) are considered operators of essential services, and will therefore, need to comply with all related cybersecurity and risk management requirements – some

[1] (ISC)². 2022. Cybersecurity Workforce Study 2022.

of them overlap with the CRA essential requirements, making compliance likely counterproductive. Additionally, some critical products listed in the Annex can be delivered both in an on-premise and in a SaaS-format. Not fully excluding SaaS from the proposed CRA would only add unnecessary complexity that might deter businesses from using cloud-based software.

In addition, Recital 10 excludes open-source software that is not used in the course of a commercial activity. Moreover, this exclusion can only be found in the recital, whereas the definition of 'making available on the market' means "any supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge", which would – to our understanding – include any type of open-source software. In this context, we urge the European co-legislators to clarify whether or not open-source software is handled in relation to the Cyber Resilience Act, and how the accountability requirements for open-source software components can be implemented in software. Moreover, open-source software must be handled in a uniform manner regardless of it being connected to co a commercial activity or not, otherwise, this will cause significant confusion.

Furthermore, German industry appreciates that the European Commission tries to prevent a double regulation of those products with digital elements for which cybersecurity requirements have been regulated by specific legislative acts. However, such exceptions from the horizontal Cyber Resilience Act should be contained to those currently listed in Article 2 point (2), (3) and (4).

Requirements for products with digital elements (Article 5 and Annex I)

German industry welcomes, that after the coming into effect of the Cyber Resilience Act, products with digital elements shall be made only available on the internal market, if they comply with a targeted list of essential requirements and if the manufacturer has put in place vulnerability handling process according to Annex I. However, as the CRA is intended to cover a wide range of heterogeneous products (e.g., kitchenware as well as Industrial Automation & Control Systems), it will be necessary that the requirements are uniformly understood by all manufacturers and that manufacturers can apply risk-adequate measures to achieve these requirements. The co-legislators should be aware that enhancing the cyber-resilience of all products with digital elements will likely lead to an increase in prices for products. However, as a risk-adequate level of cyber resilience is paramount for protecting the functioning of an increasingly connected European society, these additional costs are well invested. Nonetheless, it is important that the proposed market surveillance ensures that the European internal market constitutes a level playing field, on which all market actors can and are implementing the essential requirements set out in Annex I Section 1.

essential requirements: The list of essential requirements as proposed by the European Commission already addresses several important aspects which will augment Europe's cyber resilience. In general, the obligations should not entail excessive costs and should be limited to proportional measures based on the intended use.

In addition, the co-legislators should be more precise in their use of technical terms in Annex I. For example, instead of "known exploitable vulnerability" the European co-legislators should opt for "exploitable vulnerability known to the manufacturer". This is important, since secret services and other public bodies of the EU Member States are frequently aware of vulnerabilities, i.e. "known exploitable vulnerabilities", of which they do not inform the manufacturer. As manufacturers can only mitigate vulnerabilities of which they are aware / made aware, EU Member States and the European Union's

institutions, such as ENISA, should be obliged to share their knowledge of vulnerabilities with the respective manufacturers of products with digital elements.

The European Commission's proposal stresses that only products without any vulnerability known to the manufacturer shall be placed on the European market. A product's cyber-resilience can be influenced by numerous factors, including the product's deployment environment, the development of different technologies, and by the evolving cyber-attack landscape. Since "placing on market" for hardware products means "every single item sold", the requirement for 'delivered without any known exploitable vulnerabilities' would yield to immediate sales / delivery stop, and hence, cause huge logistics problems, additional costs if practical at all. To remediate this issue in the legal text, German industry urges the co-legislators to amend Annex I Section 1 (2) in such a way, that it directly references the vulnerability handling process of Annex I Section 2, so that a. o. it would be possible to implement an automatic update check when a product with digital elements is first connected to the internet by its end user / integrator to fulfil the essential cybersecurity requirements set out in Annex. This should be understood as current state-of-the-art." In addition, having to destroy products with digital elements that have a known exploitable vulnerability for which an update is available, but which can no longer be soled as it does not fulfil the requirement "without any known exploitable vulnerability" would not be acceptable from a sustainability-perspective. Products with digital elements that have a vulnerability, but for which an update is available and can be immediately installed at the time of their first use, should be allowed to be sold.

Moreover, we recommend allowing economic operators to implement a risk-based approach to remediating vulnerabilities based on numerous factors and situational circumstances like the vulnerability risk level and the criticality of the data and the systems impacted. Such an approach would allow manufacturers of products with digital elements to focus on remediating the most critical vulnerabilities first and would also be aligned with existing global industry standards and frameworks. For example, should a manufacturer of products with digital elements be confronted with a vulnerability in a product, whose intended use is in critical infrastructures, remediating this vulnerability could be more important than developing an update for a consumer good where the exploitation of the vulnerability has less far-reaching implications.

vulnerability handling processes: In general, German industry welcomes the proposed vulnerability handling process. It is essential that the time required for a thorough risk assessment and the search for the right remediation, i.e. developing an update / patch as well as testing and validating it is not understood as "undue delay" but rather as a technical necessity to ensure high quality updates.

Furthermore, the European co-legislators should be more precise, how often a test / review must be conducted to be understood as "regular".

Proposed changes to the legislative text:

Annex I Section 1 (2): Products with digital elements shall be delivered without any ~~known~~ exploitable vulnerabilities *known to the manufacturer. If a manufacturer of a product with digital elements ensures that the said product directly at the first time of use runs an automatic update-check and installs all available updates, it fulfils the requirements of sentence one.*

Annex I Section 1 (4): *The manufacturer shall only be obliged to fulfil the essential requirements set forth in Section 1 and 2 of Annex 1 to the extent achievable by using the best available techniques which are commercially reasonable considering, inter alia, the costs and benefit of a measure and the intended use of the product with digital elements.*

Annex I Section 2 (2): ~~in relation~~ *proportional* to the risks posed to the products with digital elements, address and remediate vulnerabilities *known to the manufacturer within a reasonable period which could depend on the criticality of the vulnerability known to the manufacturer, and which allows for testing and validating an update before making it available if applicable* ~~without delay~~, including by providing security updates;

Annex I Section 2 (4): once a security update has been made available, publically disclose information about fixed vulnerabilities *consistent with internationally accepted standards – especially CVE –*, including a description of the vulnerabilities *known to the manufacturer*, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities *known to the manufacturer*;

Annex I Section 2 (8): ensure that, where security patches or updates are available to address identified security issues, they are disseminated without undue delay *and for at least the timeframe stated in Article 6,* free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken. *By derogation from sentence one, maintenance services including the installation of updates may be subject to service fees agreed between the relevant contractual parties, if agreed on beforehand.*

Critical products with digital elements (Article 6 and Annex III)

In its proposal, the European Commission differentiates between four types of products with digital elements: products with digital elements, two classes of critical products with digital elements and yet to be defined highly critical products with digital elements. German industry appreciates this approach in principle as such a differentiation follows the necessary risk-based approach. However, German industry considers the categories of products with digital elements to be defined as “critical” class I and II, which include, for example, microcontrollers, industrial automation and control systems as well as parts of the Industrial Internet of Things, as too broad. This issue could become even more problematic, as the category of “highly critical” products could be defined in accordance with Article 6 (5) after the date of applicability of the CRA, therefore, it is currently impossible for industry to foresee the impact and the addressed products. Rather than referring to product groups in terms of “critical” or “highly critical”, the co-legislators should focus more specifically on the intended use of these products with digital elements. For example, Annex III categorises microprocessors as a “critical” product with digital elements of Class I or II. Hence, the Commission’s proposal does not sufficiently consider the intended use of these components for products with digital elements. From industry’s point of view, it makes a huge difference with regards to the criticality of the same microprocessor whether it is used within a coffee machine or a router.

Proposed changes to the legislative text:

In light of the above stated remarks, we would appreciate if the co-legislators were to change Annex III accordingly:

Class I

Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use *in critical areas of* ~~by~~ essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];

Class II

12. Industrial Automation & Control Systems (IACS) intended for the use *in critical areas of* ~~by~~ essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);

Industrial Internet of Things devices intended for the use *in critical areas of* ~~by~~ essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];

Obligations of manufacturers (Article 10 and Annex I)

German industry welcomes the European Commission's core idea that manufacturers shall only place those products with digital elements on the market that fulfil essential cybersecurity requirements, such as security-by-design and protection from unauthorised access by appropriate control mechanisms. Moreover, we appreciate that all manufacturers are required to implement, in a structured manner, a vulnerability handling process. To ensure that manufacturers of products with digital elements are made aware of all known vulnerabilities, German industry 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 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.

German industry welcomes the Commission's proposal made in Article 10 (6) that obliges manufacturers of products with digital elements to handle and mitigate vulnerabilities for the lifetime of the product or for 5 years, whichever of the two is shorter. German industry perceives this as a well-balanced approach that takes into account the requirements of very different product categories. However, as recent cyber incidents and acts of sabotage on critical infrastructures have shown, Europe's critical infrastructure is increasingly the target of malicious actors. Taking this into account, manufacturers of products with digital elements that are highly critical for the functioning of essential entities could be obliged to offer their customers remunerated service agreements that ensure that these products with digital elements receive updates and patches longer than the currently foreseen five-year-period if technologically feasible.

The obligation to provide "clear, understandable, intelligible and legible" information (Article 10 (10)) should consider the relevant addressee (e.g., IT administrator in business-to-business transactions).

Moreover, the co-legislators should clarify the intention and meaning of Annex I point 9 b "how changes to the product can affect the security of data". The current wording leaves room for interpretation regarding whose changes have an effect on the security of data.

Manufacturers should provide remedies for identified vulnerabilities within a timeframe appropriate to the significance of the vulnerability and the criticality of the product, taking the use of the product into account. For example, major security updates of products used in critical infrastructure should be provided without culpable delay. In addition, security updates may be provided as part of regular routine updates.

German industry perceives the current requirements to ensure “confidentiality of all data” (Annex 1 Section 1 (3c)) and “integrity of all data” (Annex 1 Section 1 (3d)) as too broad. Rather, the manufacturer of a product with digital elements should – as part of the risk assessment required in Article 10 (2) –assess which data are especially sensitive, and henceforth, require special protection in terms of confidentiality and integrity. Therefore, we would appreciate the insertion of “where required based on a holistic risk assessment according to Article 10 (2)” in the respective requirements.

Proposed changes to the legislative text:

In light of the above stated remarks, we would appreciate if the co-legislators were to change Article 10 accordingly:

16. Government bodies of Member States must, without undue delay, inform manufacturers of products with digital elements about any vulnerability they are aware of.

In light of the above stated remarks, we would appreciate if the co-legislators were to change Annex I Section 1 “Essential Cybersecurity Requirements” accordingly:

(c) protect*, where required based on a holistic risk assessment according to Article 10 (2),* the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;

(d) protect*, where required based on a holistic risk assessment according to Article 10 (2),* the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

Reporting obligations of manufacturers (Article 11)

The Commission’s proposal requires manufacturers of products with digital elements to notify ENISA without undue delay and in any event within 24 hours of becoming aware of it any actively exploited vulnerability contained in the product with digital elements (Article 11 point 1). German industry appreciates that manufacturers of products with digital elements shall report vulnerabilities known to the manufacturer to an EU agency rather than to the cybersecurity agencies of 27 Member States, as this will significantly reduce the bureaucratic burden caused by such notifications. However, ENISA and the competent national authorities must ensure that the reporting process under the Cyber Resilience Act mirrors as best as possible the respective structures under NIS 2. Furthermore, as gathering information is time-consuming and mitigating the vulnerability by providing a well-tested update or patch should always be the primary goal, we urge the European co-legislators to increase the reporting period to 72 hours.

The co-legislators should establish a fully digital information flow and secure reporting mechanism both to ENISA as well as between ENISA, competent national authorities, and market surveillance bodies for reports according to Article 11 point 2 for any incident having impact on the security of the product with digital elements. Manufacturers of products with digital elements should only have to report such incidents once within the EU (i.e. either to ENISA or to one Member State). Due to the massive gap in cybersecurity professionals, amounting to more than 104,000 IT security specialists in Germany

alone[2], efficient reporting mechanisms based on the once-only principle are crucial to ensure that companies can focus on incident and vulnerability handling rather than on reporting the same information to various national and EU institutions.

Proposed changes to the legislative text:

In light of the above stated remarks, we would appreciate if the co-legislators were to change Article 11 accordingly:

1. The manufacturer shall, without undue delay and in any event within ~~24~~ *72* hours of becoming aware of it, notify to ENISA any *significant* actively exploited vulnerability contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability.

1a. ENISA shall, after having consulted relevant stakeholder groups, establish a digital reporting mechanism, which enables manufacturers of products with digital elements via Application Programming Interfaces (API) and a web-based form to fulfil their reporting obligations pursuant to paragraph 1.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any *significant* incident having *a significant* impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact. *To ensure a common level of reporting, ENISA will, within 6 months after the ratification of this Regulation set out what constitutes a significant incident and a significant impact.*

3. ENISA shall submit to the European cyber crisis liaison organisation network (EUCyCLONe) established by Article [Article X] of Directive [Directive XXX/XXXX (NIS2)] information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

3a. ENISA shall forward without undue delay information notified by manufacturers of products with digital elements pursuant to paragraphs 1 and 2 to the national competent authorities for cybersecurity in an electronic format via secure channels.

Rules and conditions for affixing the CE marking (Article 22)

German industry appreciates the European Commission's proposal to show compliance with the requirements spelled out in the Cyber Resilience Act via the CE marking. The application of the CE marking has been tested and established for many years. Hence, private and commercial users

[2] (ISC)². 2022. Cybersecurity Workforce Study 2022.

recognise the compliance with corresponding requirements by the CE marking. Therefore, German industry appreciates that the European Commission does not propose to introduce an additional label.

The European co-legislators should – by all means – avoid the introduction of any kind of cybersecurity protection / risk product labels. In any case, if a Member State or the European Commission were to introduce such a label, it should not be static as the cybersecurity risk is constantly evolving.

Conformity assessment procedures for products with digital elements (Article 24)

German industry welcomes that the Commission's proposal for a Cyber Resilience Act relies on the conformity assessment procedures established by the NLF. The selected conformity assessment procedures (Module A, Module B+C and Module H) also reflect the different risk-levels of the products with digital elements falling within the directive's scope.

As the digital industry is highly innovative, which is expressed in very short product life cycles, Module H, which involves a third-party assessment, as well as Module B+C, which involves EU-type examination procedure in conjunction with conformity to EU-type based on internal production control, should only be utilised for the conformity assessment of those products with digital elements whose intended use is linked to a high degree of risk. Typically, innovation in the digital industry does not concern the entire product, but the parts of the product that ensure its core functionality as well as new features. Therefore, the time to market of a product is crucial. Hence, the involvement of an external testing body (notified body) in the implementation of the conformity assessment procedure should only be applied when necessary as the involvement of an external testing body inevitably leads to delays in market introduction (time to market) and therefore, inhibits the application of innovative solutions. If used excessively, this would have a negative repercussions for on the competitiveness of the internal market and would also lead to a considerable disadvantage in global competition. The European co-legislators must ensure that start-ups and SMEs are not confronted with additional market-entry barriers, while at the same time they have to ensure that no additional cyber-risks arise from products developed by SMEs and Start-ups.

The intended use, which is defined by the manufacturer, and the reasonably foreseeable use must be a core aspect when assigning Conformity Assessment Procedures in the framework of the Cyber Resilience Act.

From an overarching perspective, it is important to acknowledge that cybersecurity is a result of responsible design, manufacturing, and use of a product. Importantly, cybersecurity is not a static product feature (like "leak-proof"). To maintain high levels of cyber-resilience, standards and labelling should focus on secure processes rather than on (volatile) technological features.

Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk (Article 43)

German industry welcomes that the Cyber Resilience Act foresees market surveillance activities at both national and European level. What is essential, however, is and effective and overlap-free implementation of these competencies. To this end, Member States must ensure that their market surveillance bodies have employees with excellent IT security and technical know-how. As Europe – as all parts of the world – experiences a significant shortage of these professionals, market surveillance bodies will only be able to employ such experts if they can pay competitive wages. At the same time, an effective market surveillance is integral for the effective and efficient implementation of the Cyber Resilience Act. Otherwise, manufacturers of products with digital elements that do not implement the

essential requirements pursuant to Annex I section 1 and the vulnerability handling procedures according to Annex I section 2 will be able to place their products on the internal market at much lower prices than those who fulfil the respective requirements and implement the respective procedures. This would give the former a significant competitive advantage in relation to the latter.

Therefore, we urge the European co-legislators to agree on a longer implementation period of 36 months. Such a longer implementation period is paramount, as it will enable the European Commission to issue a standardisation request, the manufacturers to ensure CRA-conformity of their products and process, and the market surveillance bodies to recruit employees and set up necessary organisational structures.

Furthermore, the market surveillance bodies of the 27 Member States and ENISA must ensure an effective coordination amongst themselves. In addition, fines by multiple market surveillance bodies for the same reason must be excluded.

Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk (Article 45)

In addition to the remarks made above (cf. Article 43), the Commission, if it intends to delegate new tasks to ENISA, the EU's cybersecurity agency must also receive more employees. If the von der Leyen Commission, the European Parliament and Member States wish to enhance Europe's cyber-resilience reshuffling tasks and competencies within ENISA's staff – amounting to 120 persons – will not do the trick. Rather, ENISA urgently requires a significant increase of its head count.

Formal non-compliance (Article 47)

Private and commercial users recognise the compliance with corresponding requirements by the CE marking. As a CE marking as well as related conformity and technical documentation provide respective manufacturers of products with digital elements with a competitive edge, German industry welcomes that market surveillance authorities in the EU Member States will control the formal compliance with the conformity marking, the EU declaration of conformity and the technical documentation. As the Radio Equipment Directive (RED) includes as additional items under formal non-compliance "product identification, manufacturer identification, importer information, information on intended use", German industry would appreciate if these aspects were added as types of formal non-compliance under CRA as well, as they are not all covered under 'technical documentation'. It must be ensured that market surveillance authorities have sufficient financial and personnel resources to fulfil their related tasks.

Penalties (Article 53)

In order to ensure that all manufacturers, importers and distributors fulfil requirements according to articles 10, 11, 13 or 14 respectively relating to the essential requirements and the procedures on vulnerability handling according to Annex I, as well as the articles relating to the cooperation with market surveillance bodies, the introduction of fines is justified. In general, German industry perceives the differentiation according to three types of misconduct proposed as acceptable.

Proposed changes to the legislative text:

3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15 000 000

EUR or, if the offender is an undertaking, up to 2.5 % of ~~the~~ its total worldwide annual turnover for the preceding financial year, whichever is *lower* ~~higher~~.

4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is *lower* ~~higher~~.

5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is *lower* ~~higher~~.

Entry into force and application (Article 57)

German industry welcomes the European Commission's intention to increase Europe's cybersecurity holistically. The Cyber Resilience Act adequately complements the requirements introduced by the NIS 2-Directive. However, German industry believes that the implementation period of 12 to 24 months is too short to implement the essential requirements across all products with digital elements according to Article 2 (1). This is the case, as the Cyber Resilience Act constitutes the first regulatory act on the European internal market to horizontally regulate the cyber resilience of products. Consequently, companies across sectors have to review their internal measures for CRA-conformity / or even have to set up respective measures, and have to implement a vulnerability handling mechanism that accommodates the requirements set out in Annex I Section 2. In this regard, the Commission's proposal does not sufficiently consider the significant amount of work that manufacturers of (critical) products with digital elements might have to conduct in order to be compliant with the CRA's essential requirements as well as the vulnerability handling process. Especially supply-chain related requirements will necessitate manufacturers to closer cooperate with their software suppliers and / or the open-source software community. Moreover, the Member States have to organise the market surveillance outlined in Article 43. To this end, new organisational structures have to be defined and new employees have to be hired. Furthermore, harmonised European norms have to be developed – either from scratch or based on IEC 62443. To this end, the European Commission has to issue the standardisation request. All this will take more than the proposed 12 to 24 months. Henceforth, we urge the European co-legislators to prolong the implementation period to 36 months.

Proposed changes to the legislative text:

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [~~24~~ *36* months after the date of entry into force of this Regulation]. ~~However Article 11 shall apply from [12 months after the date of entry into force of this Regulation].~~

Software Bill of Materials (SBOM) (Annex I Section 2 Point 1)

SBOM as a 'stand-alone concept' does not add much value. It needs to be part of an overall standards-based concept documenting details of the software but limited to essential information. ISO/IEC 5962:2021 and Cyclone-DX already address SBOMs rather well. Nonetheless, SBOMs are still in their infancy, and as such, have not yet achieved the required maturity level on how they should be implemented, shared and used. Therefore, it will be critical to ensure that regulators allow and support the

private sector to coalesce on the standard-based concepts and formats that work best for given industries and organisations.

SBOMs should use standard-based and machine-readable formats integrated in an overall concept to support their uptake. The industry is already significantly investing in accelerating the maturation of SBOM standards and best practices. It is therefore crucial to encourage the private sector to continue developing new standard-based concepts and formats that work best for given industries and organisations, and for regulators to ensure close industry consultation when defining SBOMs requirements.

Secure software design, development, build, and distribution practices are well understood and defined in many industry standards and guidelines and have been for years. Software development organisations typically do not need to invent new approaches to solve security aspects. Instead, they should focus on using and executing such well-established practices like described in the ISO/IEC 20243 standard, as well as the NIST Secure Software Development Framework (SSDF), for example, as the foundation for its security-by-design practices.

SBOMs are only useful if developers actually rely on them to identify and address vulnerabilities in dependency chains throughout the software development lifecycle rather than treat them merely as a reporting requirement.

Imprint

Federation of German Industries / Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobby Register: R000534

Editor
Steven Heckler
Deputy Head of Department Digitalisation and Innovation
T: +49 30 2028-1523
s.heckler@bdi.eu

BDI Document Number: D 1691