# Cyber Resilience Act - end of the regulator's patience

## CRA unfolds effect on non-regulated actors.

Holger Friedrich
Dr Waldemar Grudzien
Leon Kuhlmann

February 2023
Blogpost

## Key Facts

- European harmonization of security requirements for "products with digital elements" (hardware and software) is to be welcomed.
- The primary objective of the regulation is to oblige manufacturers to "seriously" concern themselves with security throughout the entire life cycle of a product.
- The aim of the CRA Regulation is to increase product security; enforcement requires adjustments to market realities as well as geostrategically changed framework conditions.
- In some cases, importers and distributors are subject to considerable security obligations.
- Requirements will overburden smaller and medium-sized economic actors, reactions in the market currently not assessable.
- Businesses and business associations should intensify lobbying to make regulation implementable not only for big players.
- In terms of impact, the CRA Regulation is the counterpart to the Supply Chain Act at the beginning of the supply chain, with a market-clearing effect.

## Introduction

The EU is gradually intensifying and completing its digital legislation. With the Cyber Resilience Act (CRA) in the draft version of 16 September 2022, the European Data Strategy, which is based on the four pillars of data protection, fundamental rights, safety, and cybersecurity, is strengthened in the fourth pillar. The principles of product liability are extended to hardware and software products, in the language of the CRA "products with digital elements".

With the CRA, the EU stimulates the optimization of two major challenges in the European Single Market: A structurally low level of cybersecurity and the insufficient understanding of and access to cybersecurity information by users.

With the aim of supporting the European Single Market, two overarching objectives have been set:

1) The creation of conditions for the development of secure products with digital elements in order to place hardware and software products with fewer vulnerabilities on the market, complementing that manufacturers are held responsible for security for the full life cycle of a product, and

2) creating conditions that enable users to take cybersecurity into account when selecting and using products with digital elements.

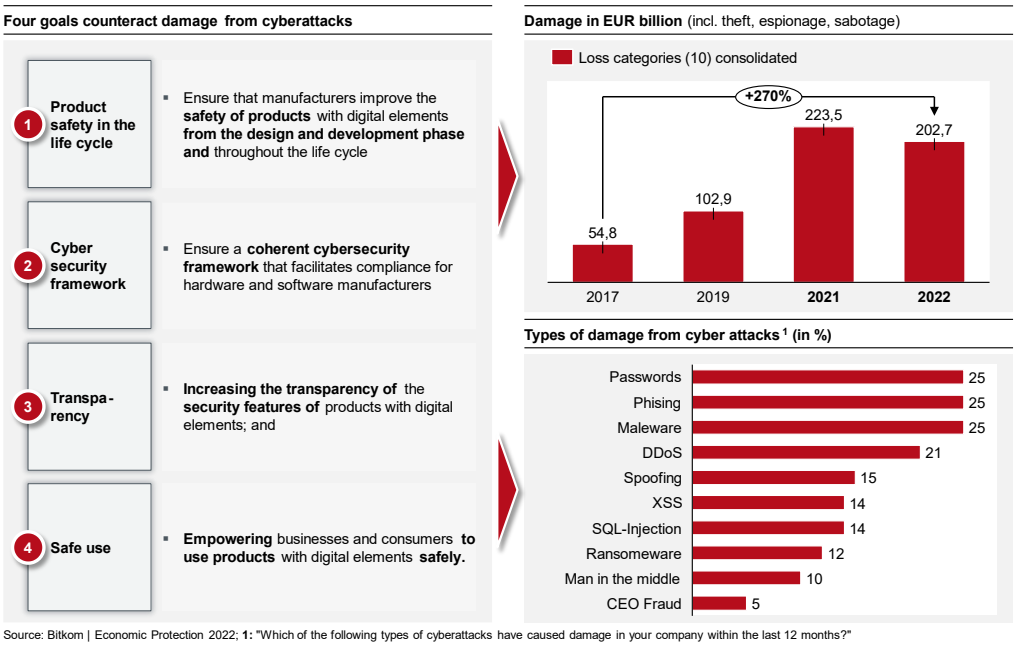



Figure 1: German economy affected by attacks across the board and expects increased cyberattacks

To this end, four specific objectives have been subordinated:

i. Ensure that manufacturers improve the security of products with digital elements from the design and development phase and throughout the lifecycle,

ii. Ensure a coherent cybersecurity framework that facilitates compliance for hardware and software manufacturers,

iii. Increasing the transparency of security features for products with digital elements; and

iv. Empowering businesses and consumers to use products with digital elements safely.

Figure 1 illustratively plots the four specific targets mentioned above against the damage and damage types from successful cybersecurity attacks over time since 2017.

The primary objective of the CRA is thus a manufacturer obligation for "products with digital elements" to ensure security "seriously" (recital 2) during the complete life cycle of a product. In addition, importers (distributors) and retailers are subject to security obligations. The need to strive to achieve the objectives of the CRA is shown by Figure 2 which shows the need for protective measures in anticipation of "strong and rather increasing cyberattacks". The high level of adaptation of the CRITIS sectors (84%) is striking and positive.

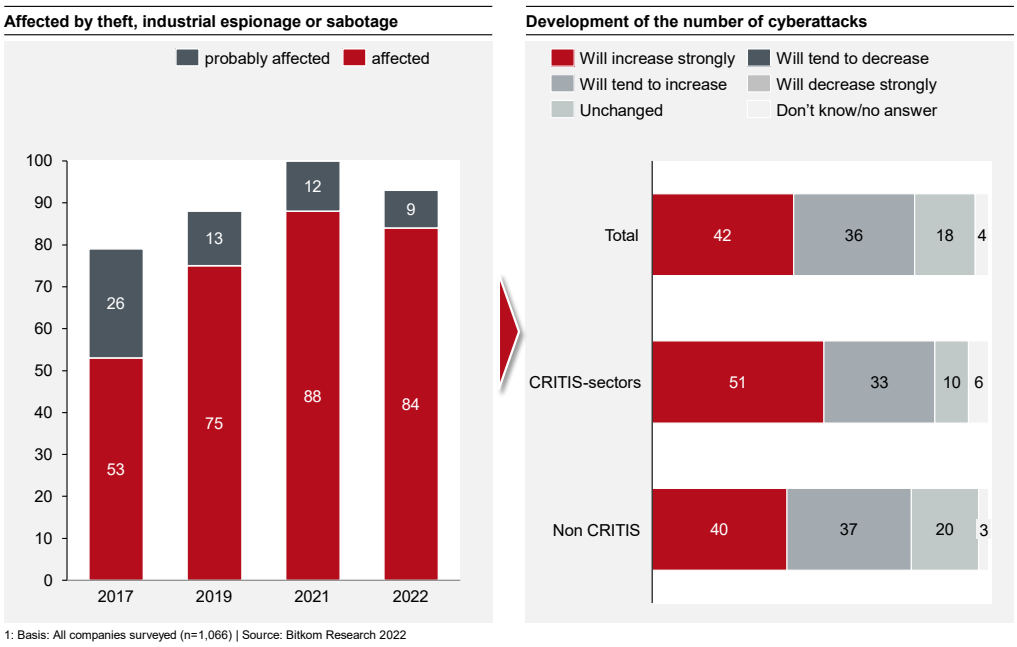



Figure 2: CRA targets are intended to counteract damage caused by cyber-attacks (theft, espionage, sabotage, etc.).

## Technical analysis

The regulatory content of the Cyber Resilience Act (CRA) is shown in Figure 3. In the following, the chapters of the CRA are discussed in detail, or in a cursory manner in the case of already known issues. Articles that require supplementary efforts, such as security requirements for economic actors, supplementary administrative efforts to existing regulations and others, are analysed in detail. This procedure is due to the fact that the scope of regulations, such as the

European conformity regulation (CE mark) of Chapters 3 and 4, is sufficiently common practice in the economy.

**Cyber Security Act Com (2022) 454 - Regulatory content**

| Chapter | Title | Article |
|---|---|---|
| 1 Chapter I | General provisions | Article 1 to Article 9 |
| 2 Chapter II | Obligations of economic operators | Article 10 to Article 17 |
| 3 Chapter III | Conformity of the product with digital elements | Article 18 to Article 24 |
| 4 Chapter IV | Notification of conformity assessment bodies | Article 25 to Article 40 |
| 5 Chapter V | Market surveillance and enforcement | Article 41 to Article 49 |
| 6 Chapter VI | Delegated powers and committee procedures | Article 50 to Article 51 |
| 7 Chapter VII | Confidentiality and sanctions | Article 52 to Article 53 |
| 8 Chapter VIII | Transitional and final provisions | Article 54 to Article 57 |

Source: CORE

Figure 3: Regulatory content of the Cyber Security Act COM(2022) 454, version of 16.09.2022

**Article 1** defines the "subject matter" of the CRA for products with digital elements in four cybersecurity requirement groups:

a) Rules for placing on the market
b) Requirements for conception, development and production
c) Basic requirements for the treatment of vulnerabilities
d) Rules for market surveillance and enforcement of requirements.

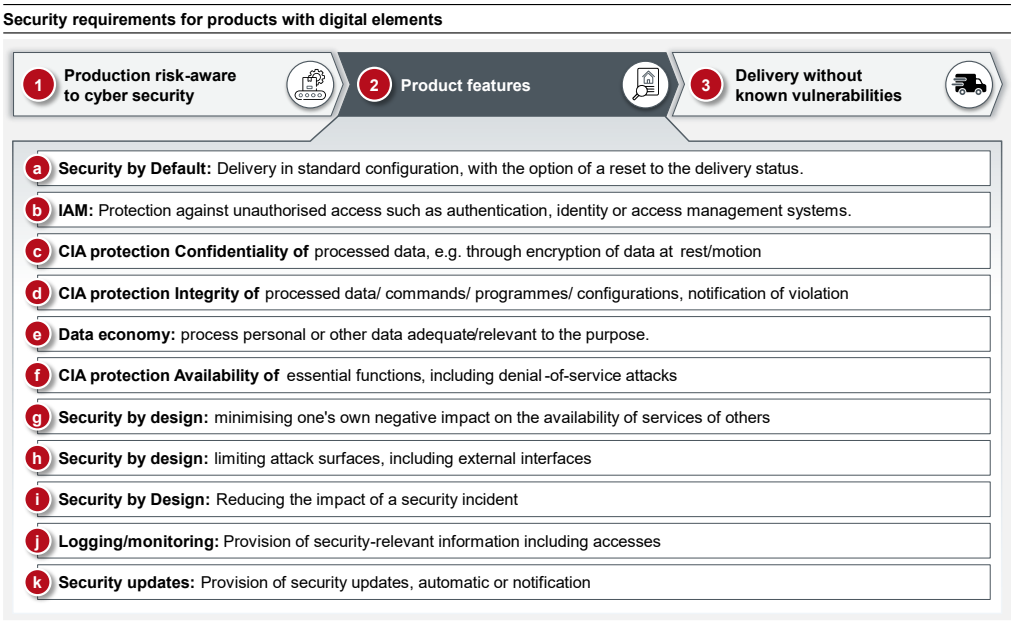
**Article 2** "Scope" specifies which products fall within the regulatory framework of the CRA and which do not: the former group includes products with digital elements whose "intended or reasonably foreseeable use involves a direct or indirect logical or physical connection to a device or network". In practical terms, this means that all products with a network interface are included.

Products to which other Union acts apply are not covered by the CRA: Medical devices, in vitro diagnostic medical devices, motor vehicles and civil aeronautical products. Paragraph 4 provides that the application of the Regulation may be limited or even excluded to products with digital elements covered by other EU legislation with a similar affinity of risk and achieving the same level of protection. According to paragraph 5, the Regulation does not apply to products containing digital elements designed exclusively for national security or military purposes, nor to products specifically designed for the processing of classified information. Here, the member states reserve the right to their national security - a clear reference to solving the Privacy Shield challenges in the context of the first amendment of the GDPR.

**Article 4** "Free circulation" paragraph 3 offers a new business model for the abuse of warning letters: software that does not comply with this regulation (for testing purposes, only available for a limited period of time) must have a "visible marking" "that it does not comply with this regulation".

**Article 5** opens the tableau of "requirements for products with digital elements" to be fulfilled. These may only be made available on the market if, according to No. 1, they meet the essential requirements in Annex I, Section 1 (security requirements, see Figure 4) and on condition that they are properly installed, maintained and used for their intended purpose or under reasonably foreseeable circumstances and, where appropriate, updated.

The second part of Article 5 No. 1 - "properly installed, maintained and used for its intended purpose or in reasonably foreseeable circumstances and, where appropriate, updated" - is aimed at Annex II (information and instructions for users, see Figure 5 right-hand side)).

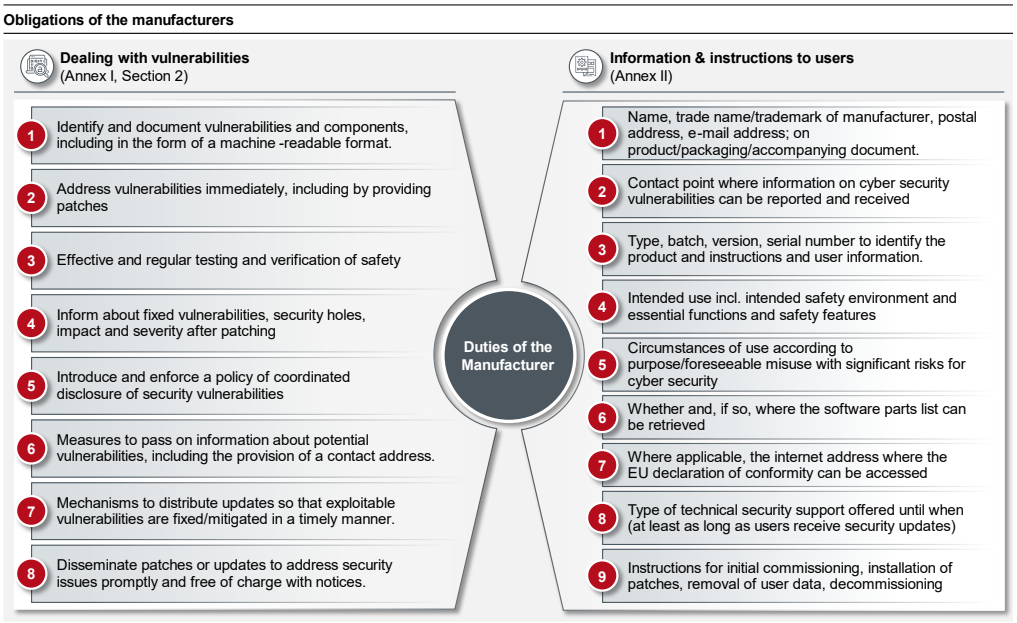



Source: CORE

Figure 4: Security features of products with digital elements (Annex I, Section 1)

The security features for design, development and production compiled in the eleven letters "a" to "k" form the Who's Who of IT product security as well as data protection and have been demanded by politicians and consumer protectionists for years: CIA protection, security by design and by default, IAM, data economy, logging/monitoring and patching. Considering Annex III, this is an ambitious package. The risks arising from use must be matched by appropriate measures to ensure cybersecurity.

According to Annex I Section 1 paragraph 2, products with digital elements must be delivered without known exploitable vulnerabilities. For unknown vulnerabilities, Annex I Section 2 sets out eight requirements for dealing with them (Figure 5 left side). For further assistance, manufacturers must provide users with information and instructions on products with digital elements (Annex II) (Figure 5 right side).




Source: CORE

Figure 5: Dealing with vulnerabilities in products with digital elements and information and instructions for users

**Article 6** applies to "Critical Products with Digital Elements". These are listed in Annex III with their core functions, divided into two classes I and II and thus two cybersecurity risk classes. Paragraph 2 gives the EU Commission the right to make changes to the list by determining the level of cybersecurity risk of a potential candidate for the list based on various criteria:

- Cybersecurity function and at least one of the features
  - i) Increased privileges/administration of privileges.
  - ii) Direct or privileged access to network or computing resources.
  - iii) Access control to data/operational technology.
  - iv) Function crucial for trust/especially security function (network control, endpoint security, protection of the network)
- Is subject to the NIS-2 Directive

- is subject to the GDPR
- Impairment of a large number of persons (quantity criterion of persons affected from data protection)
- Losses, disruptions, significant concerns in the past

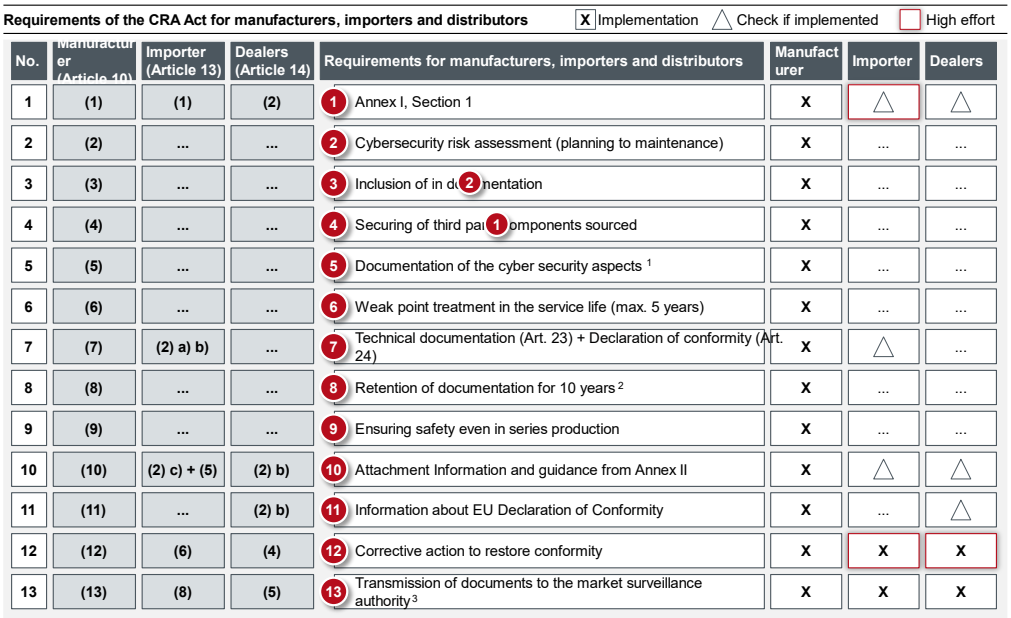
According to paragraph 4, critical devices are subject to the conformity assessment procedures set out in Article 24(2) (Class I) and (3) (Class II). Class I critical devices can claim a presumption of conformity according to Article 18. This is denied to Class II critical devices and they must immediately undergo an EU type-examination procedure or a conformity assessment.

A question arises regarding Class I No. 13 "Remote access/sharing software": According to recital 9, SaaS[1] offers do not fall within the regulatory framework of the CRA, but of the NIS-2 Directive. However, SaaS offers are addressed by the CRA via the aforementioned No. 13. The EU Commission should provide clear clarification here. Open-source software is clearly excluded by recital 10: free and open source software that is developed and provided outside of a business activity as well as software for testing purposes (recital 21) are also not covered by the CRA.

In the last paragraph 5, the EU Commission reserves the right to define categories for highly critical products with digital elements. Manufacturers would have to obtain cybersecurity certification for these products under a European system in accordance with the Cyber Security Act. Articles 7 to 9 deal with the interaction of the Cyber Resilience Act with regulations for other product categories: general product security for products not subject to the CRA (Article 7), high-risk AI systems regulated by the AI Regulation (Article 8) and machinery products within the scope of the Machinery Products Regulation (Article 9).

Chapter II "Obligations of economic operators" with **Articles 10 to 17** represents the central catalogue of requirements of the Regulation. Article 10 (obligations of manufacturers), Article 13 (obligations of importers) and Article 14 (obligations of distributors) result in a total of 23 combined obligations for these three economic operators (see Figure 6 and Figure 7). It should be noted that importers and distributors not only have to verify that manufacturers have fulfilled their obligations, but in some cases also have to carry out active verification actions themselves in order to meet requirements.

[1] Software-as-a-Service



**Requirements of the CRA Act for manufacturers, importers and distributors** — X Implementation — △ Check if implemented — □ High effort

| No. | Manufacturer (Article 10) | Importer (Article 13) | Dealers (Article 14) | Requirements for manufacturers, importers and distributors | Manufacturer | Importer | Dealers |
|---|---|---|---|---|---|---|---|
| 1 | (1) | (1) | (2) | 1 Annex I, Section 1 | X | △ | △ |
| 2 | (2) | ... | ... | 2 Cybersecurity risk assessment (planning to maintenance) | X | ... | ... |
| 3 | (3) | ... | ... | 3 Inclusion of in d 2 nentation | X | ... | ... |
| 4 | (4) | ... | ... | 4 Securing of third pa 1 omponents sourced | X | ... | ... |
| 5 | (5) | ... | ... | 5 Documentation of the cyber security aspects [1] | X | ... | ... |
| 6 | (6) | ... | ... | 6 Weak point treatment in the service life (max. 5 years) | X | ... | ... |
| 7 | (7) | (2) a) b) | ... | 7 Technical documentation (Art. 23) + Declaration of conformity (Art. 24) | X | △ | ... |
| 8 | (8) | ... | ... | 8 Retention of documentation for 10 years [2] | X | ... | ... |
| 9 | (9) | ... | ... | 9 Ensuring safety even in series production | X | ... | ... |
| 10 | (10) | (2) c) + (5) | (2) b) | 10 Attachment Information and guidance from Annex II | X | △ | △ |
| 11 | (11) | ... | (2) b) | 11 Information about EU Declaration of Conformity | X | ... | △ |
| 12 | (12) | (6) | (4) | 12 Corrective action to restore conformity | X | X | X |
| 13 | (13) | (8) | (5) | 13 Transmission of documents to the market surveillance authority [3] | X | X | X |

Source: CORE | 1: incl. vulnerabilities, updating of documentation if required | 2: according to the EU Declaration of Confor mity | 3: to prove conformity

Figure 6: Combined obligations of the economic operators manufacturer, importer and distributor - list 1 to 13

Some examples are used to explain the active audit actions of importers and distributors:

- Figure 6, number 1:
  - Article 10(1): Manufacturers must ensure that the product has been designed, developed, and manufactured in accordance with the essential requirements set out in Annex I, Section 1.
  - Article 13(1): importers must verify that products meet the essential requirements set out in Annex I(1) and that the procedures adopted by the manufacturer meet the essential requirements set out in Annex I(2).
  - Article 14(2): distributors have lesser obligations in this task
- What does the inspection order to the importers mean? Does it mean a target-target check, i.e. checking the manufacturer's documentation, or does it mean a target-actual check, i.e. actively checking whether what the manufacturer claims in the documentation actually applies. In the second case, the question must be allowed as to which importers are able to do this and how many importers will remain on the market.
- Figure 6, number 12:
  - Article 10(12): Manufacturers shall immediately take the corrective measures necessary to restore conformity or, if appropriate, to withdraw or recall the product in cases of non-compliance.
  - Article 13(6): Importers must "take" the necessary corrective measures without delay.
  - Article 14(4): Distributors "shall" ensure that the necessary corrective measures are "taken without delay".
- What do the orders mean for importers and distributors? Does an importer have to take corrective action on its own, such as a recall or informing users of identified vulnerabilities? How many importers can realistically do this? Distributors also have to ensure that appropriate measures are taken. In case of doubt, this requirement means a triple check of every product

with digital elements, as importers and distributors cannot rely on the information provided by the manufacturers, but have to check every product themselves in the light of the information provided by the manufacturers.

**Requirements of the CRA Act for manufacturers, importers and distributors** X Implementation △ Check if implemented ☐ High effort

| No. | Manufacturer (Article 10) | Importer (Article 13) | Dealers (Article 14) | Requirements for manufacturers, importers and distributors | Manufacturer | Importer | Dealers |
|---|---|---|---|---|---|---|---|
| 14 | (14) | (9) | (6) | 14 Information to market surveillance authority in case of discontinuation of operation | X | X | X |
| 15 | (15) | ... | ... | 15 EU-COM may define elements of the software bill of materials | ... | ... | ... |
| 16 | ... | (3) | ... | 16 Inform. to market surveillance authority in case of cyber security risks | ... | X | ... |
| 17 | ... | (4) | (2) b) | 17 Contact details of the importer | ... | X | △ |
| 18 | ... | (5) | ... | 18 Annex II in an easy language for users | ... | X | ... |
| 19 | ... | (6) Part 1 | (4) Part 1 | 19 Non-compliance with Annex I leads to corrective action (recall) | ... | X | X |
| 20 | ... | (6) Part 2 | (4) Part 2 | 20 Information to manufacturer and market surveillance authority[1] | ... | X | X |
| 21 | ... | (7) | ... | 21 Keeping the documentation and the EU declaration of conformity available | ... | X | ... |
| 22 | ... | (8) | (5) | 22 Provision of all information to market surveillance authority2 | ... | X | X |
| 23 | ... | ... | (1) | 23 Observing the Cyber Resilience Act with "due diligence". | ... | ... | X |

Source: CORE | 1: Information to manufacturer on vulnerabilities and to market surveillance authority on cybersecurity risks and corrective actions | 2: should this be so requested

Figure 7: Combined obligations of economic actors manufacturers, importers and distributors - Enumeration 14 to 23

- Figure 7, number 20
  - Article 13(6) (Part 2) / Article 14(4) (Part 2): If a vulnerability is identified in the product with digital elements, importers / distributors shall immediately inform the manufacturer of that vulnerability. Furthermore, where the device with digital elements presents a significant cybersecurity risk, importers / distributors shall immediately inform the market surveillance authorities of the Member States in which they made the device with digital elements available on the market, giving details, in particular, of the non-compliance and of any corrective action taken.
- And also in the third example, it must be asked which importers and which distributors can identify vulnerabilities as well as significant cybersecurity risks; in addition, set up a regulatory process for reporting to the market surveillance authorities and operate it as a line process as well as take their own corrective action up to and including a recall.

**Article 10**(10) provides a point of attack for the warning industry if a manufacturer does not comply with all the requirements of Annex II.

The reporting obligations formulated in **Article 11** are new for manufacturers. These are well known to the financial industry as an example but are new and thus a multi-dimensional challenge for the majority of manufacturers of products with digital elements. In Figure 8 is an iconic compilation of the reporting obligations.

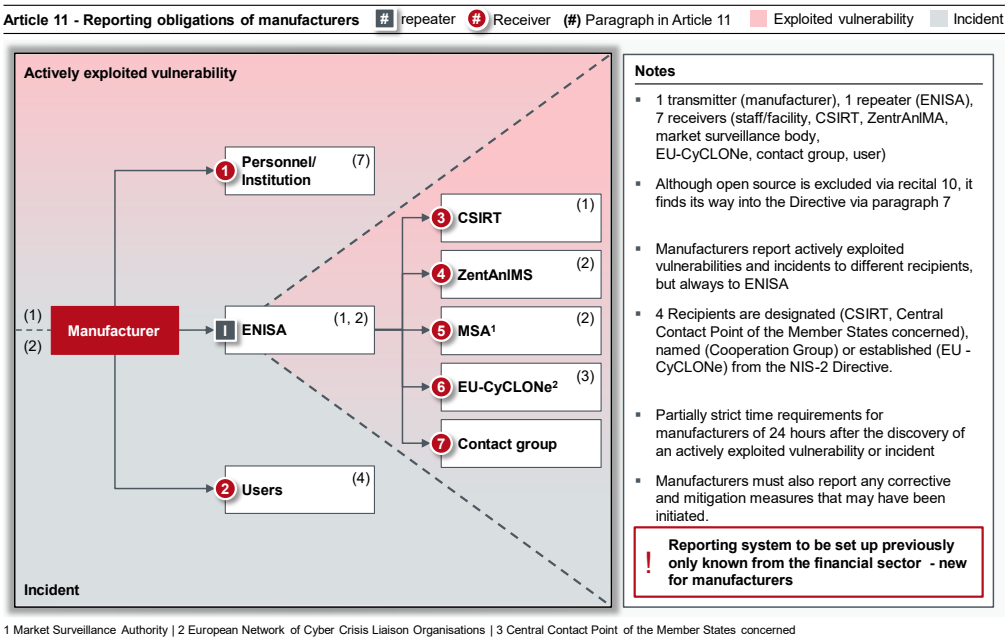



Figure 8: Reporting obligations of manufacturers under Article 11

Among other things, manufacturers must report actively exploited vulnerabilities (paragraph 1) or incidents (paragraph 2) to ENISA within 24 hours. ENISA shall report to the CSIRTs[2] of the Member States concerned. If the information from (1) and (2) is relevant for the management of massive cybersecurity incidents and crises at operational level, manufacturers must report this from paragraph 3 to EU-CyCLONe[3]. Finally, in paragraph 4, end-users also play a role: manufacturers must inform them of measures they can take to remedy the situation. ENISA must submit a technical report on cybersecurity risk trends to the Cooperation Group every two years (paragraph 6). Paragraph 7 has an interesting twist: although open source is excluded via recital 10, it finds its way into the directive here because "as soon as the manufacturer identifies a vulnerability in a component integrated into the product with digital elements, including an open source component, it shall report the vulnerability to the person or entity maintaining that component".

What does this requirement mean exactly? An "open-source component" that is integrated into the product can only be a software artefact. This would mean that open source software would also be affected, whether directly from the manufacturer or as a supply to his product. And in order to be able to report a vulnerability in a component, the manufacturer must check all the open source software used.

In Chapter II, **Article 17** "Identification of economic operators" defines request situations. Upon request, manufacturers, importers and distributors must provide the market surveillance authority with information on the sources of supply as well as on the recipients of the products and remain able to provide this information for 10 years. The purpose of the regulation is the detailed presentation of a structural analysis of all components and products from the manufacturer and

[2] Computer Security Incident Response Team
[3] European Network of Cyber Crisis Liaison Organisations

his sources of supply to the distributors and - if possible - all their recipients over a period of 10 years. Although this period sounds long for the usual life cycles of attack patterns, considering the partly widespread legacy in many infrastructures, the 10 years are well chosen to manage exploitable vulnerabilities and incidents.

Chapter III "Conformity of the product with digital elements" consists of Articles 18 to 24 and should start with the last Article, because **Article 24** sets out the mechanics for establishing conformity. If the manufacturer determines that his product is a product with digital elements according to Article 2, he must carry out a conformity assessment. Three procedures are available for this purpose:

a) Internal control procedure (according to Annex VI Module A) or
b) EU type-examination procedure (according to Annex VI Module B) or
c) Conformity assessment (according to Annex VI Module H)

Where the product is a critical product as defined in Article 6, only two procedures (b) or (c) may be used. This applies in the case of an Annex III Class I device with presumption of conformity and in the case of an Annex III Class II device without presumption of conformity as referred to in **Article 18**. This presumption of conformity shall be conferred where the device and the procedures adopted by the manufacturer are in conformity with harmonized Union standards or parts thereof, insofar as those requirements are covered by those standards or parts thereof. Conformity shall also be presumed in the case of compliance with common specifications referred to in **Article 19** and with an EU declaration of conformity or a cybersecurity certificate in accordance with the Cybersecurity Directive.

The EU declaration of conformity issued by the manufacturer himself (model in Annex IV) states that the essential requirements in Annex I are met. For this proof, the conformity assessment procedure according to Article 24 has to be passed through. All three conformity assessment procedures (Annex VI Module A, Module B or Module H) require a technical documentation according to **Article 23**. This documentation is demanding because it requires "at least" the information from Annex V. Among other things, this includes

- Paragraph 2c): complete information and specifications on the production and monitoring of the product and the validation of these processes.
- Paragraph 3: an assessment of the cybersecurity risks against which the product is designed, developed, manufactured, delivered and maintained in accordance with Article 10
- Paragraph 5: Test reports to verify the conformity of the product and the procedures for dealing with vulnerabilities with the applicable essential requirements in Annex I
- Paragraph 7: where applicable, the software parts list as defined in point 37 of Article 3, upon a reasoned request from a market surveillance authority, where this is necessary for that authority to verify compliance with the essential requirements.
- may verify in accordance with Annex I

The technical documentation must be updated during the product's lifetime, but at least 5 years. Here too, the question is which manufacturers can realistically afford this bureaucratic effort?

Chapter IV "Notification of Conformity Assessment Bodies" with **Articles 25 to 40** deals with the requirements for notification bodies, both notifying authorities and notifying bodies.

Chapter V "Market surveillance and enforcement" (Articles 41 to 49) still has some interesting aspects: **Article 43**, for example, describes national procedures for products with digital elements that pose a significant cybersecurity risk in order to ultimately withdraw these products from the market. **Article 45** describes the same procedure at EU level. That is, both a Member State and the EU may withdraw products from the market in case of imminent danger. **Article 44** provides a link between the two procedures with the "Union safeguard clause procedure", because it offers a Member State and the Commission the possibility to intervene in another Member State on products in case of imminent danger. Even if a product is compliant with the CRA, it can be removed from the market if a significant cybersecurity risk arises under **Article 46**. The last article of Chapter V introduces so-called "coordinated controls (sweeps)", whereby market surveillance authorities may decide to carry out simultaneous coordinated controls ("sweeps") to check compliance with the CRA or to detect breaches of the CRA. Here, the actual application of the CRA in about three years remains to be seen. Cooperation between several market surveillance authorities is well known in the financial sector, with BaFin and the Bundesbank successfully working together on examinations of the technical and organizational equipment of a German supervisory object; in the case of "significant" institutions, this coupling is supplemented by the ECB. The extent to which such European-coordinated examination and monitoring activities will be used for products with digital elements remains to be seen in the future.

With regard to the sanctions under **Article 53,** the CRA borrows from the GDPR both in terms of the amount of the fines and the type of infringements. While the GDPR has two fine ranges, the CRA even has three:

- Failure to comply with the essential requirements set out in Annex I or failure to comply with the obligations set out in Articles 10 (obligations of manufacturers) and 11 (notification obligations of manufacturers): Fine of up to 15 million euros or up to 2.5% of the total annual worldwide turnover, whichever is higher
- Breaches of other obligations: Fine of up to 10 million euros or up to 2% of total annual worldwide turnover, whichever is greater
- False, incomplete or misleading information provided to notified bodies and market surveillance authorities upon their request for information: Fine of up to 5 million euros or up to 1% of the total annual worldwide turnover, whichever is higher.

If it is not a mistake in the draft, then the third fine with the naming of the notifying "bodies" (and not notifying "authority") offers a door to denunciation for malicious bodies. Here, too, practice must be awaited; for an auditing company will realize prompt reactions in the market in the case of unclean behavior towards manufacturers.

Only companies can be fined. However, according to Article 53(8), each Member State shall adopt rules on whether and to what extent fines may be imposed on public authorities and public bodies established in that Member State. Following the experience with other legal acts, this is decided negatively in Germany. The last paragraph 10 of Article 53 states that, depending on the

circumstances of the individual case, fines may be imposed in addition to other corrective measures or restrictive measures imposed by market surveillance authorities for the same infringement.

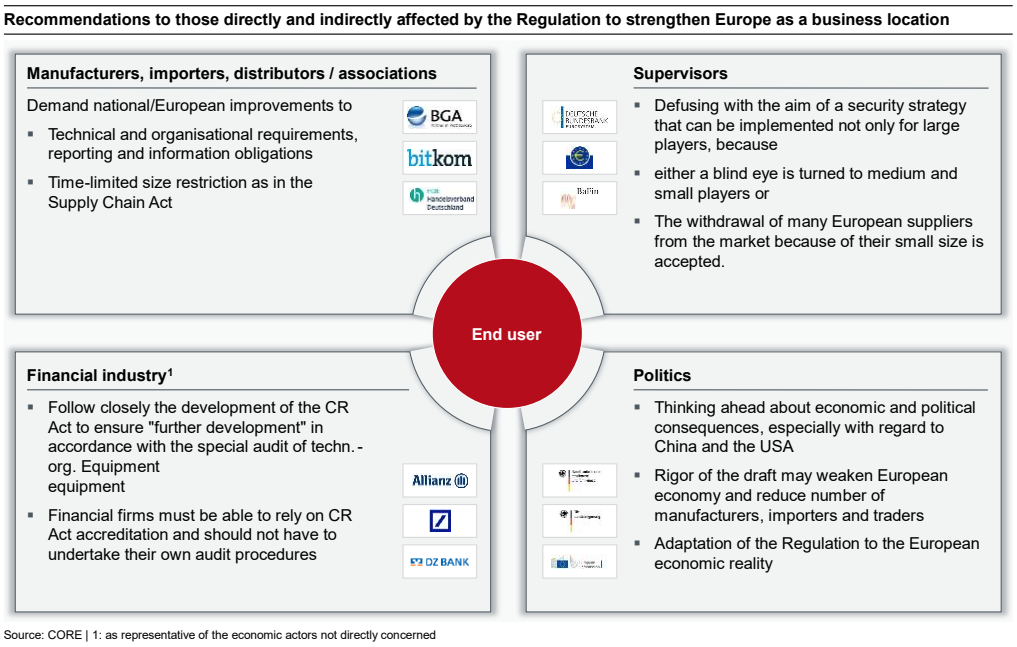
Finally, entry into force and start of application (**Article 57**): this starts 2 years after the entry into force of the CRA, only the notification obligations of manufacturers (Article 11) start already one year after entry into force. If viewed benevolently, this bringing forward of the reporting obligations can be interpreted as a learning phase for manufacturers in dealing with the CRA.

## Recommendations

Our recommendations, summarized in Figure 9 and subsequently expanded upon, apply to the four main economic actors addressed in the regulation: the business associations, the national and European supervisory authorities, the economic actors not directly affected, such as the financial industry, as well as German and European policymakers.

1) In our opinion, manufacturers, importers and distributors should work towards improvements to the regulation through their business associations, both nationally and at the European level. These improvements concern the technical and organizational requirements. The technical requirements from Annex I will tend to be manageable only by larger and large players. Many manufacturers will also not be able to adequately implement the additional administrative workload in the reporting system and the information obligations in Annex II and Annex V. In addition, there are various storage and information obligations described above at the request of various authorities.
2) In addition, the addressees should introduce at least a time-limited size restriction for manufacturers, importers and distributors along the lines of the Supply Chain Act into the discussion with regulators and politicians. Otherwise, with the application of the regulation, a large number of economic actors will act non-compliant with the regulation - with corresponding risks of sanctions.

3) Furthermore, the market players must prepare themselves promptly for the regulation and start implementing the requirements. The path can only be outlined here: Gap analysis for the regulation, planning of measures, migration plan, implementation, checking for conformity. There is still enough time for all parties involved, probably at least 3 years until the application of the CRA.
4) In our opinion, the national and European supervisors should also tone down the regulation as described above. The goal should be an implementable security strategy, not a set of rules that could only be lived by large players. Either the supervisory authority will act with restraint, at least in the first few years, in the case of medium-sized and small players - there is no reference to size limits as in the Supply Chain Act - or the withdrawal of many and primarily European, because small, providers from the market will have to be accepted. A circumstance that European policymakers should discuss.
5) Economic actors not directly affected, such as the financial industry, should also follow the development of this regulation and, if necessary, intervene in the development of the law at an early stage. Because from the current audit practice of credit institutions and insurance companies, a possible "further development" of the supervisory practice for financial companies can be derived as follows:



Source: CORE | 1: as representative of the economic actors not directly concerned

Figure 9: Recommendations to those directly and indirectly affected by the Regulation to strengthen Europe as a business location

In the CRA there are articles for the obligations of the actors manufacturer (Article 10), importer (Article 13) and distributor (Article 14). However, there is no article "Obligations of users". In the end, financial companies are also only users of products with digital elements, i.e., hardware and software. Therefore, the following deduction: Today, a bank in outsourcing must control and monitor as closely as if it continued to operate systems under its own responsibility. This is true even if the outsourcing companies themselves have all the important security certifications and operational certifications. The financial supervisory authority insists on its own audit procedures of the objects of supervision. Similarly, manufacturers of products with digital elements must comply with many new requirements from the regulation. What happens when financial

companies use these products? Can they rely on the CRA approval, or must they carry out their own audit procedures? If one transfers today's situation in financial supervision to the future with the CRA, the financial companies will also have to check this product type themselves: an additional effort that can hardly be calculated. It would be the continuation of today's supervisory situation, for example, from special audits of the technical and organizational equipment. A permissible question from the supervisory authority to financial institutions would be: "Have you checked the manufacturer's cybersecurity risk assessment yourself?" This obligation to conduct its own audits despite compliance with the CRA would not be limited to manufacturers but would also include the actions of importers and distributors. Financial firms should pre-emptively avoid this possible broadening of supervisory practice, as otherwise the regulatory burden will increase incalculably.

German and European policy should react to the industrial policy tableau between the USA and China, taking geopolitical changes into account. This means revising the regulation under economic and political consequences for the European economic area. Does this rigor in the application of the regulation, i.e. without size barriers for regulated companies and with high requirements from the beginning for all companies, contribute equally to strengthening European companies in the market? A second possible effect of the regulation could be the further reduction of the number of manufacturers, importers and distributors, since in this "survival of the fittest" only larger, globally active market participants can correspond. Do politicians really want to further restrict the European economy, which tends to rely on medium-sized and small structures in this area? Or should the regulation not be specifically adapted to European industrial policy realities? Following the principle that the same rights and obligations apply to all companies but adapted to European requirements.

The Commission expects "any compliance costs for companies to be outweighed by the benefits of higher levels of security for products with digital elements and ultimately higher levels of user confidence in those products." But larger market players will find it easier to comply. Unfortunately, few of the larger market players are based in Europe.

## Conclusion

The contents of the CRA have been demanded by politics and consumer protection for decades and have been postponed again and again. What has been tried and failed to be achieved on a goodwill basis is now reflected in the draft text. Although the goal of the regulation is not in doubt, the roadmap should be discussed in detail with those directly and indirectly affected. The goal of European harmonized product safety should not be achieved at the price of damaging the software and hardware industries, which will become more important in the future.

Requirements such as cybersecurity risk assessment, reporting of actively exploited vulnerabilities to ENISA, European vulnerability database, informing users about incidents and, if necessary, corrective actions, documentation of products (including software parts lists), simultaneous coordinated controls (sweeps) are to be welcomed, but should not overburden smaller manufacturers, importers and distributors.

The main addressees must already start preparing for the implementation of their respective obligations today, approx. 3 years before the application of the CRA. Here, too, policymakers

should examine whether obligations for importers and distributors lead to excessive demands. The regulation, which is correct in itself, would become ineffective if the addressees cannot ensure implementation and withdraw from the market.

Economic actors such as the financial industry must also examine the draft and, if necessary, become involved in the political dialogue. Today's supervisory practice with required internal audit procedures in outsourcing suggests that the regulator is demanding the audit of the application of the CRA out of a risk assessment.

In this respect, companies should lobby directly and through their national and European associations. Optimizations that could be discussed include company size limits as in the Supply Chain Act, stretching the measures to be implemented over time as in the DORA with the Regulatory Technical Standards (RTS) spread over time and generally thinking more deeply about updated information and reporting obligations. With the present draft, it cannot be ruled out that the CRA acts as a "counterpart" of the Supply Chain Act and pushes small and medium-sized enterprises out of the market by imposing too high requirements - only the large enterprises would remain as regulatory objects for the CRA, just as currently only large market participants are for the Supply Chain Act.

It doesn't have to come to that. There is enough time. If an optimization process kicks in, the draft CRA is already a big hit.

**Holger Friedrich** is Managing Partner of CORE SE. He has many years of experience as a successful expert in the transformation of complex IT systems. His many years of experience for international clients in regulated industries make him a sought-after contact for investors, supervisory bodies and senior management.

**Mail: holger.friedrich@core.se**

**Dr Waldemar Grudzien** is an Expert Partner at CORE SE. He is a proven specialist for regulation and compliance aspects in the use of business-critical infrastructures. Due to the large number of publications, mandates, and successful projects, he and his teams are sought-after contacts for users of highly regulated IT systems.

**Mail: waldemar.grudzien@core.se**

**Leon Kuhlmann** is Transformation Director at CORE. With his "international business" background and experience in agile and classic project management as well as knowledge of IT security, process management and compliance, he supports clients in the implementation of complex IT transformations. His focus ranges from strategy development to go-live.

**Mail: leon.kuhlmann@core.se**

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zurich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se