



MY NOTES MIGHT BE A BIT UNCLEAR

THESE NOTES WERE TAKEN WHEN I DIDN'T HAVE
SLIDES YET

Regulation of the EU: consider the roots of this act. Why did we adopt it?

Main problem outlined is that the national market was flooded by unsecure connected prod. Initially this product was highlighted in the 2nd Cybersec Strategy in 2017, partially addressed with the EUCC framework in the CS act. Still addressed in the 2020 CS strategy, that reasoned on the production of possible CS measures for connected products, that resulted in the proposal of the CS RA. Before the EU legislators adopted a vertical approach, addressing the issue from a sectorial standpoint, by addressing the pieces of legislation in the field of product security in the "New Legislative Framework" that only included minimal cybersec requirements.

Another approach was targeting specific equipments like the 2014 Directive on radio equipment with essential security requirements,

Cyber Resilience act: 15/09/2022

The screenshot shows a presentation slide with the following content:

(Connected) products cybersecurity

With a view to addressing – in the short run – the overall level of cybersecurity of connected devices, the regulatory approach adopted by the Commission, from 2019 ca., revolved around the inclusion of minimum cybersecurity requirements in the directives and regulations of the 'New Legislative Framework' (NLF), that is, product safety legislation, through the adoption of delegated acts of the Commission or a revision of the legislative instrument in question.

The Commission looked at Directive 2014/53/EU on radio equipment (RED); the Delegated Regulation EU 2022/30 specify to which categories or classes of radio equipment (e.g., wearables, etc.) the essential requirements set out in Article 3(3)(d), (e) and (f) RED apply

Moreover, EU Commission started the revision process of the General product safety directive and Machinery directive by proposing two regulations anew

↓
→ data protection
network
prov.

The goal is to include in these legal acts cybersecurity-related essential requirements

- 2) Measures we had basically provided a fragmental framework.
- 3) Connected products increased the chance of attack to affect possibly an entire supply chain.

PROBLEM: legislation was impacting only minor categories. We want a broader scope for our regulations.

26.07

Controllo Contenuti Chat Partecipanti Mano Reazioni Vista Stanze App Altro Webcam Microfono Condono

(Connected) products cybersecurity: the CRA

POSSIBILI CAUSE

- 1) Allow level of cybersecurity of products with digital elements, due to widespread vulnerabilities and insufficient provision of security patches; ①
- 2) Lack of understanding and limited access to cybersecurity information by users of products with digital elements ②

PROBLEMI

Hardware and software products are increasingly subject to cyber attacks, affecting an entire organisation or supply chain

CAUSA

Most hardware and software products (especially 'non-embedded' software) are currently not (comprehensively) covered by any EU legislation with regard to their cybersecurity

CYBER RESILIENCE ACT PROPOSAL

GOALS

- i) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle; ③
- ii) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers,
- iii) enhance the transparency of security properties of products with digital elements,
- iv) enable businesses and consumers to use products with digital elements securely.

- ① Cybersecurity requirements were not present: a producer was not required to be up to specific requirements. This caused liability problems.
- ② Most consumers didn't have the awareness to understand what they needed to do.
- ③ We will see to which products this directive applies.

37.14

Controllo Contenuti Chat Partecipanti Mano Reazioni

(Connected) products cybersecurity: the CRA

Scope

applies to

products with digital elements made available on the market whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network

does not apply to

products with digital elements to which Regulation (EU) 2017/745; Regulation (EU) 2017/746; Regulation (EU) 2019/2144; Directive 2014/90/EU apply (Aviation, medical prod...)

products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139

- products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information;

- spare parts to replace identical components in PDEs manufactured according to the same specifications

application of the CRA may be limited or excluded

products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I

where such limitation or exclusion is consistent with the overall regulatory framework applying to those products

where the sectoral rules achieve the same level of protection as the one provided for by this Regulation

Commission can adopt delegated acts specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation

* Products of digital elements: They will be covered by resilience act.

(Connected) products cybersecurity: the CRA

Scope

applies to

products with digital elements made available on the market whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network

any software or hardware product including its remote data processing solutions, and software or hardware components to be placed on the market separately (Art. 3(1))

- Hardware products and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- Software products and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- Non-commercial projects, including open source in so far as a project is not part of a commercial activity
- Services, in particular cloud/Software-as-a-Service – covered by NIS2
- Outright exclusion (cars, medical and in-vitro devices, certified aeronautical equipment, marine equipment)

Per ulteriori informazioni

*₁ Rep. included in those regulation provide for a sufficient level of protection

Manufacturers will have to comply within 10 years.

IT Laws - Sessioni - Sistemi di gestione della sicurezza - CRA - (Connected) products cybersecurity: the CRA

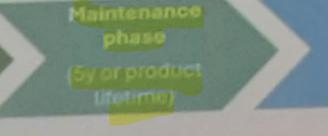
Controllo Contenuti Chat Partecipanti Muro Risposte Vista Storia App Altro Webcam Microfono Riattiva microfono

(Connected) products cybersecurity: the CRA

Obligations of manufacturers



Design and development phase



Maintenance phase
(by or product lifetime)



Post

Reporting obligations to continue

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

1. Product related ER (Annex I, Section I)
2. Vulnerability handling ER (Annex I, Section II)
3. Documentation requirements (Annex II)

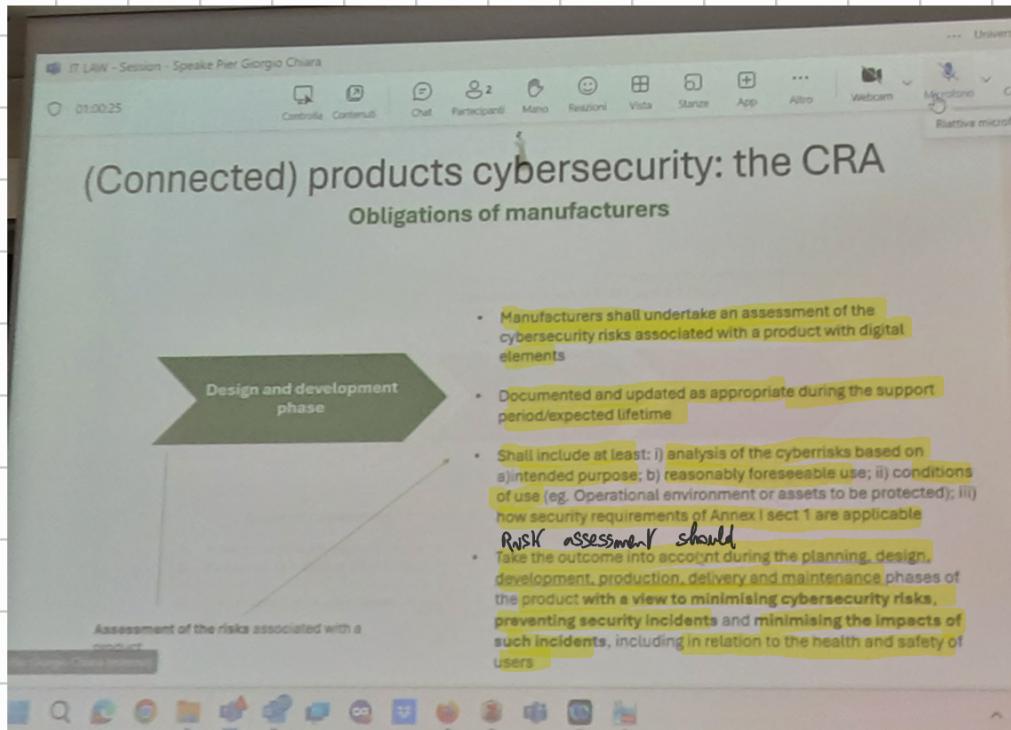
Assessment of the risks associated with a product

NOTE: The exclusion is there because of other safety or security measure in those sectors. This is done to avoid increasing the burden to producers for additional

checks to be performed. There might already be a lot of controls for certifications. Taken for granted that for specific SWs/HW's, those requirements already exist.

Obligations: not only manufacturers, also for importers, distributors, third parties that make something available on the market etc.

• Everything starts with RISK ASSESSMENT: the Gde. Res. Act, works on a risk based approach.



RISK ASSESSMENT

↓
DOCUMENTATION AND UPDATES DURING THE LIFETIME

↓
RISK ANALYSIS BASED ON INTENDED, FORESEEABLE USE; CONDITIONS OF USE

↓
TAKE ACTION IN PLAN, DESIGN, DEVELOP, PRODUCTION, DELIVERY, MAINTAINANCE

The act specifies a minimum baseline of elements to be taken into account for the risk assessment of a product.

This risk based approach is the overall framework: the first one to shift the approach and put the effort and accountability falls on the producer was GDPR. You are in charge of what are the risks and the measures. It will be up to the manufacturer to prove that they evaluated the risks and took the measures. There's no need for previous auth. System that relies on knowledge and responsibility of the manufacturer.

The slide is titled '(Connected) products cybersecurity: the CRA' and focuses on 'Obligations of manufacturers'. It highlights the 'Design and development phase'.

- Product-related ER:**
 - Designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks;
 - On the basis of the risk assessment, shall be made available without known significant risks; made available with a secure by default configuration;
 - ensure that vulnerabilities can be addressed through security updates; shall ensure protection from unauthorised access by appropriate control mechanisms;
 - shall protect the confidentiality of processed personal or other data by means of state-of-the-art measures, etc.
- Vulnerability handling ER:**
 - Identification and documentation of vulnerabilities and components contained in the product, including by drawing up a software bill of materials (SBOM) in a commonly used and machine-readable format covering at the very least the top-level dependencies;
 - Notification of vulnerabilities without delay, including by providing security updates;
 - The application of effective and regular tests and reviews of the security of the product;
 - The public disclosure of information about fixed vulnerabilities, once a security update has been made available, etc.
- Documentation requirements regarding handling vulnerabilities and information provided by third parties:**
 - Technical documentation to be drawn up by the manufacturer before the product is placed on the market and to be kept at the disposal of the market surveillance authorities for ten years after the product has been placed on the market (Art. 10, 23 and Annex V)
 - Information and instruction to the user (Annex II)
 - Shall include the risk assessment

Other sections visible on the slide include 'Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)' and 'Category'.

High level Essential Requirements: Section 1 vs Section 2 in Annex 1

Information that must be disclosed is not confidential wrt any terms

The slide is titled '(Connected) products cybersecurity: the CRA' and focuses on 'Obligations of manufacturers'. It highlights the 'Design and development phase'.

A note states: 'In the context of the Cybersecurity Resilience Act, the "presumption of conformity" refers to a legal assumption that a product meets specific cybersecurity requirements when it complies with certain established standards or certifications. If a product follows these recognized standards, it is presumed to be in line with the Act's requirements, thus simplifying the process of proving compliance.'

The slide lists several obligations:

- Presumption of conformity:** products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards (in the EU QJ) / common specifications (via EC Implementing acts); for which an EU statement of conformity or certificate has been issued under a ECCS shall be presumed to be in conformity with the essential requirements set out in Annex I
- EU declaration of conformity:** fulfilment of the applicable essential requirements set out in Annex I has been demonstrated (simplified>internet address to the full DoC)
- Conformity assessment of the PDE and the processes to determine whether the ERs are met:**

Conformity assessment options shown in a grid:

Category	Assessment Type
SELF or 3rd-PARTY ASSESSMENT/EC	SELF or 3rd-PARTY ASSESSMENT
HTB or 3rd-PARTY ASSESSMENT	HTB or 3rd-PARTY ASSESSMENT
3rd-PARTY ASSESSMENT or ECCS	3rd-PARTY ASSESSMENT or ECCS
ECCS or 3rd-PARTY ASSESSMENT	ECCS or 3rd-PARTY ASSESSMENT
Any procedure & doc made available	Any procedure & doc made available

Below the grid, it says 'DEFAULT' and 'CATEGORY'.

Other sections visible on the slide include 'CE marking' and 'Chapter IV: Member States designate a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment and notification of conformity assessment bodies and monitoring of notified bodies'.



In the Cybersecurity Resilience Act, "harmonised standards" and "common specifications" are tools used to ensure consistent cybersecurity requirements across the EU:

1. **Harmonised Standards:** These are standards developed by European standardization organizations, such as CEN, CENELEC, or ETSI, in response to a request from the European Commission. When a product complies with a harmonised standard, it is presumed to meet the relevant requirements set out in the legislation. These standards help ensure that cybersecurity practices are consistent and widely adopted across different industries.
2. **Common Specifications:** If harmonised standards are not available, insufficient, or unsuitable for certain cybersecurity needs, the European Commission can adopt common specifications. These are detailed technical requirements that serve as an alternative means of demonstrating compliance with the Act's requirements. Common specifications provide a fallback option, ensuring that there are always clear guidelines for achieving cybersecurity resilience, even when harmonised standards are lacking.

Once a product is presumed to comply the manufacturer can self certify the fulfillment of the Annex I requirement and that the req. have been demonstrated.

FOSS: lighter approach: manufacturer can choose any procedure to demonstrate compliance, they just have to make the doc. available.

Common specifications are a safety net when nothing is on the market.
Cert schemes can emerge, but they require time to be adopted. Not many available. "As a commission I will set up basic draft of specifications". Those are a safety net.

Common criteria can be used to catch part of the cyber resilience act.

Once a product is presumed to comply they can offer a EU declaration of conformity. We have a taxonomy of product scopes, with different categories and different rules. For the fifth category (not import nor critical) self assessment for compliance is okay. Default categories. If a product is considered important, depending on the criticality we have 2 classes, for lower or higher cybersecurity risks. For class I no self assessment, rely on harmonised technical standards if present, otherwise 3rd party for the evaluation. For class II rule is rely on 3rd party or EU cert schemes. Critical products present even higher possible risks. There will usually be possible updates on requirements. Still ECSS not available. Finally Foss, manufacturers can choose any procedure as long as the rules are made available.

After this manufacturers can apply the CE marking.

The slide has a green header bar with various icons and the number '01:38:27'. The main title is '(Connected) products cybersecurity: the CRA' with a subtitle 'Obligations of manufacturers'. A large green arrow points from left to right, labeled 'Maintenance phase (5y or product lifetime)'. The content is organized into several sections:

- Manufacturers inform users of the product about the incident/vulnerability and about corrective measures to be deployed to mitigate the impact of the incident. CSIRTS may provide such info to users if manufacturer fail to provide said info in a timely manner.**
- Continued compliance with vulnerability handling ER (Annex I, Section 2)**
- Obligation to report to CSIRT and ENISA via single reporting platform:**
 - 1. exploited vulnerabilities
 - 2. Severe Incidents having an impact on the security of the product
- Maintenance phase (5y or product lifetime)**
- Manufacturers report the vulnerability to the person or entity manufacturing or maintaining the component (including open-source) affected by the vulnerability integrated in the product.**
- If manufacturers 'fix' components' vulnerability, they have to share the fix to the entity responsible for the component**
- + Voluntary reporting: manufacturers/other natural or legal persons may notify any vulnerability/incident to CSIRT or ENISA**

A red annotation on the right side of the slide reads: 'legal person a report ↑ with objective of fostering security' and 'COOPERATION!'.

At the bottom left, it says 'Same obligations as NIS 2'.

Molen ns That vulnerability is a knowl. case: you are aware of a problem. knowing that it exists is a step forward to the solving of a problem. The vulnerab. might also come from parts of your device: molen ns to ensure the right info flowing chain. Same with vulnerability reporting, goes hand in hand with NIS 2.

The Cybersecurity act was covering EE, IE and supply chain, but everything outside was left behind. This goes in the direction of ensuring a high level of security for all products!

(Connected) products cybersecurity: the CRA Market Surveillance and Enforcement

National market surveillance authorities (MSAs)—designated by Member States—carry out market surveillance in that Member State.

MSAs under the CRA shall cooperate with: ENISA (technical advice); other MSAs designated on the basis of other Union harmonisation legislation for other products; national cybersecurity certification authorities designated under the CSA and DPAs.

- Joint activities between MSAs can be carried out with the aim of ensuring cybersecurity and protection of consumers
- MSAs may decide to conduct simultaneous coordinated control actions ("sweeps") of particular products to check compliance with the CRA

POWERS If a product does not comply with the CRA, MSA shall without delay require the relevant operator to take all appropriate corrective actions to bring the product into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period.

PENALTIES MSs to set rules on penalties but: i) noncompliance with Annex I ERs and Art. 10 and 11 obligations administrative fines 15M EUR/2.5% total worldwide annual turnover; ii) noncompliance with any other obligations 10M/2%; and, iii) incorrect, incomplete or misleading information to notified bodies and MSAs 5M/1%