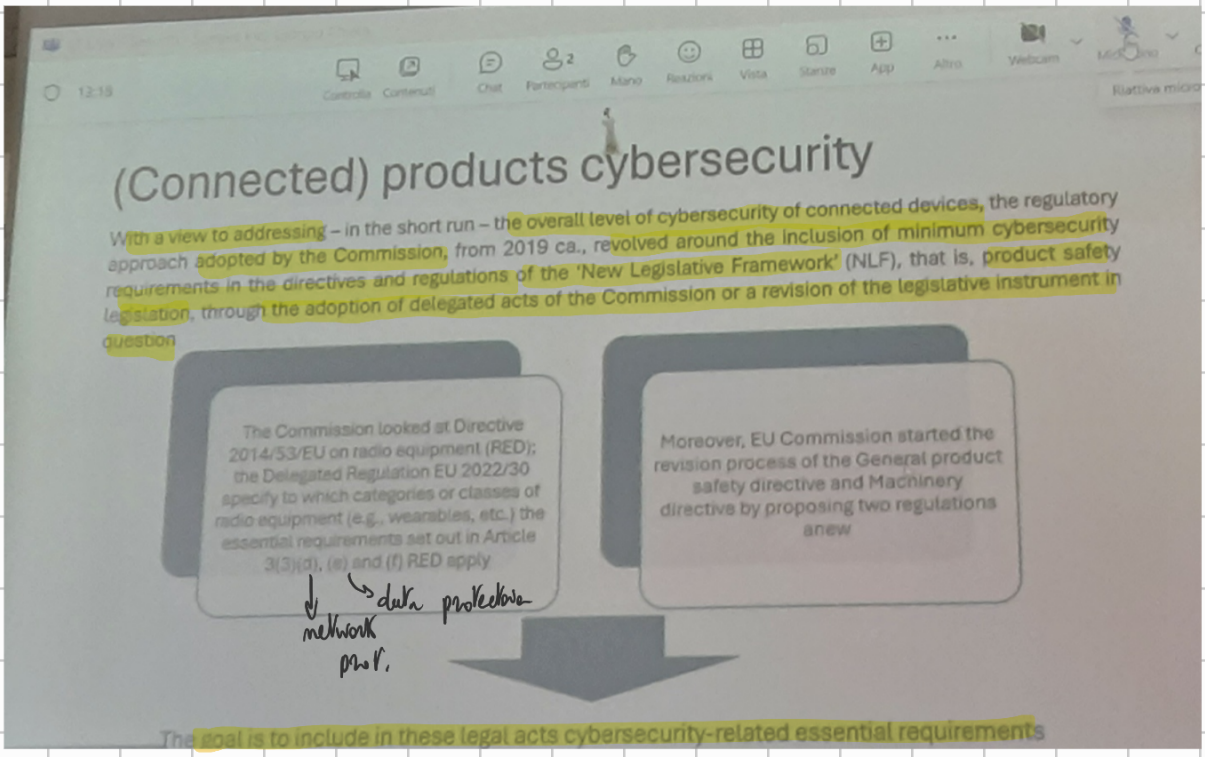
⚠ MY NOTES MIGHT BE A BIT UNCLEAR

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 aimed to tackle was the fact that internal 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

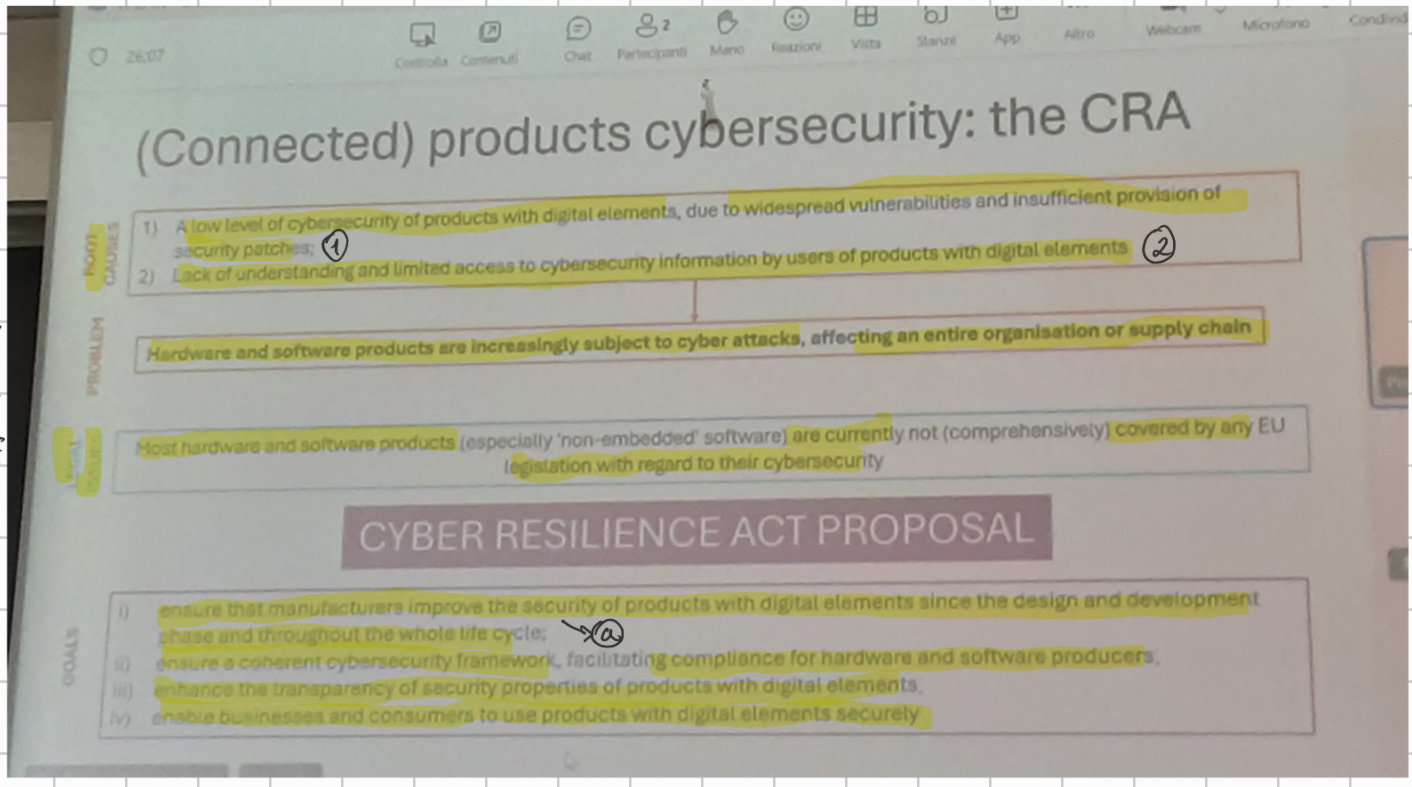


2) Measures we had basically provided a fragmental framework.

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 bigger scope for our legislations.

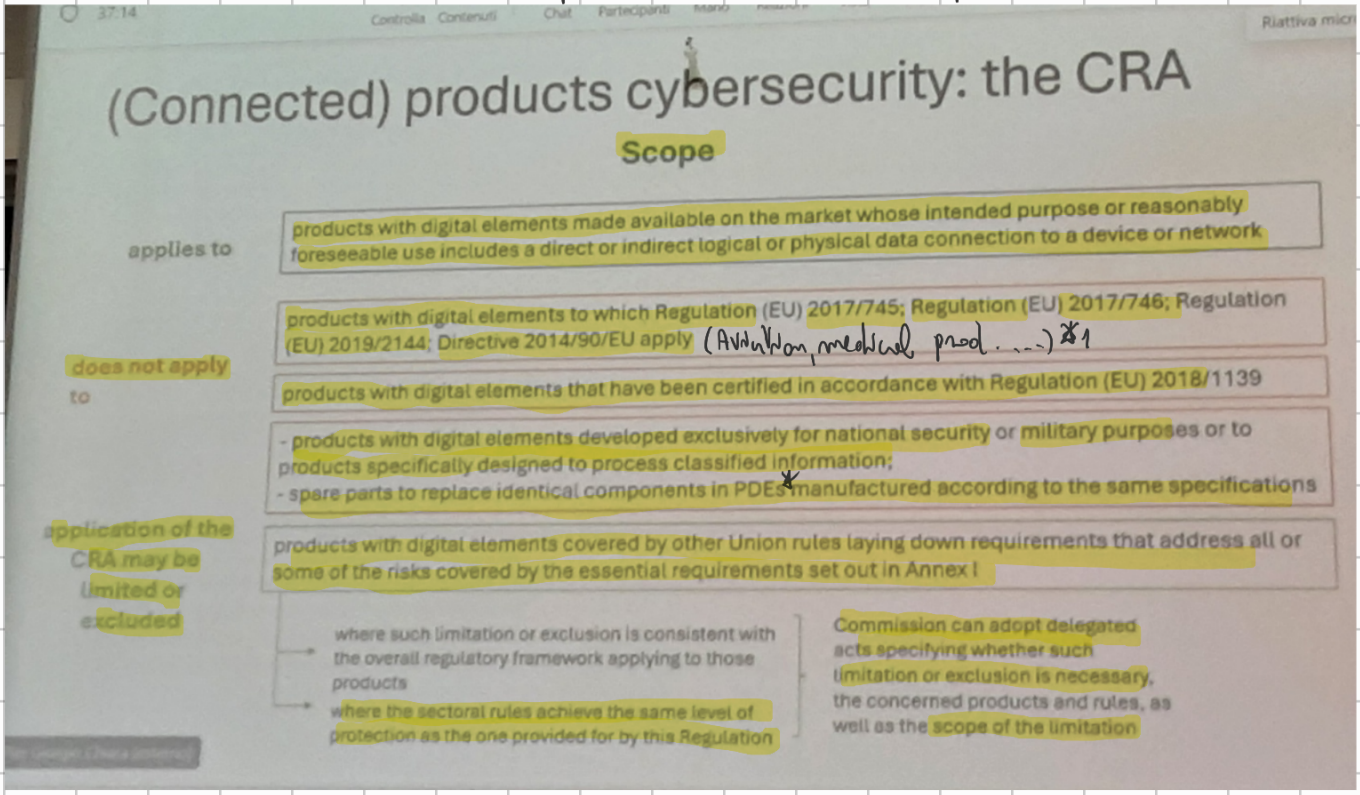
LEGAL ISSUES



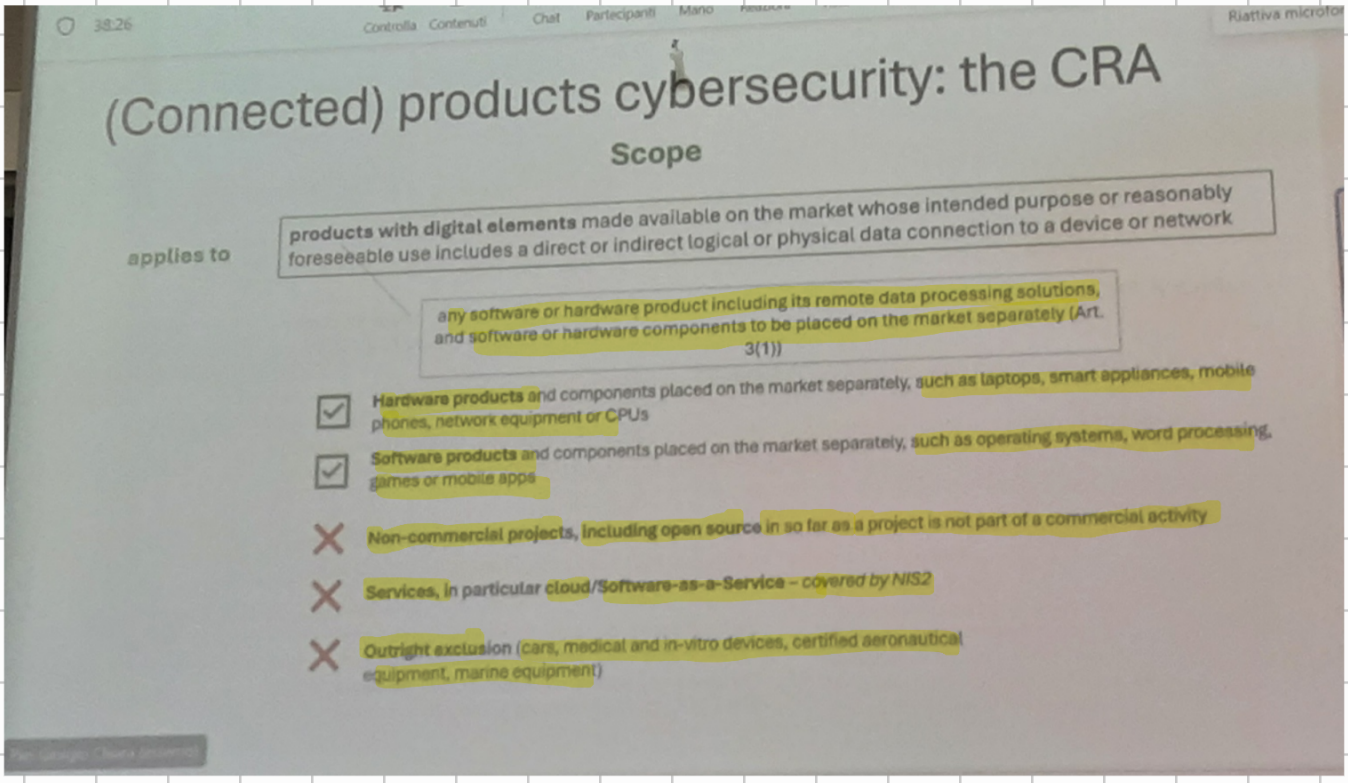
① Cybersecurity requirements were not present: a producer was not required to be up to specific requirements. This caused liability problems.

② Most consumers didn't have the awareness to understand what they needed to do.

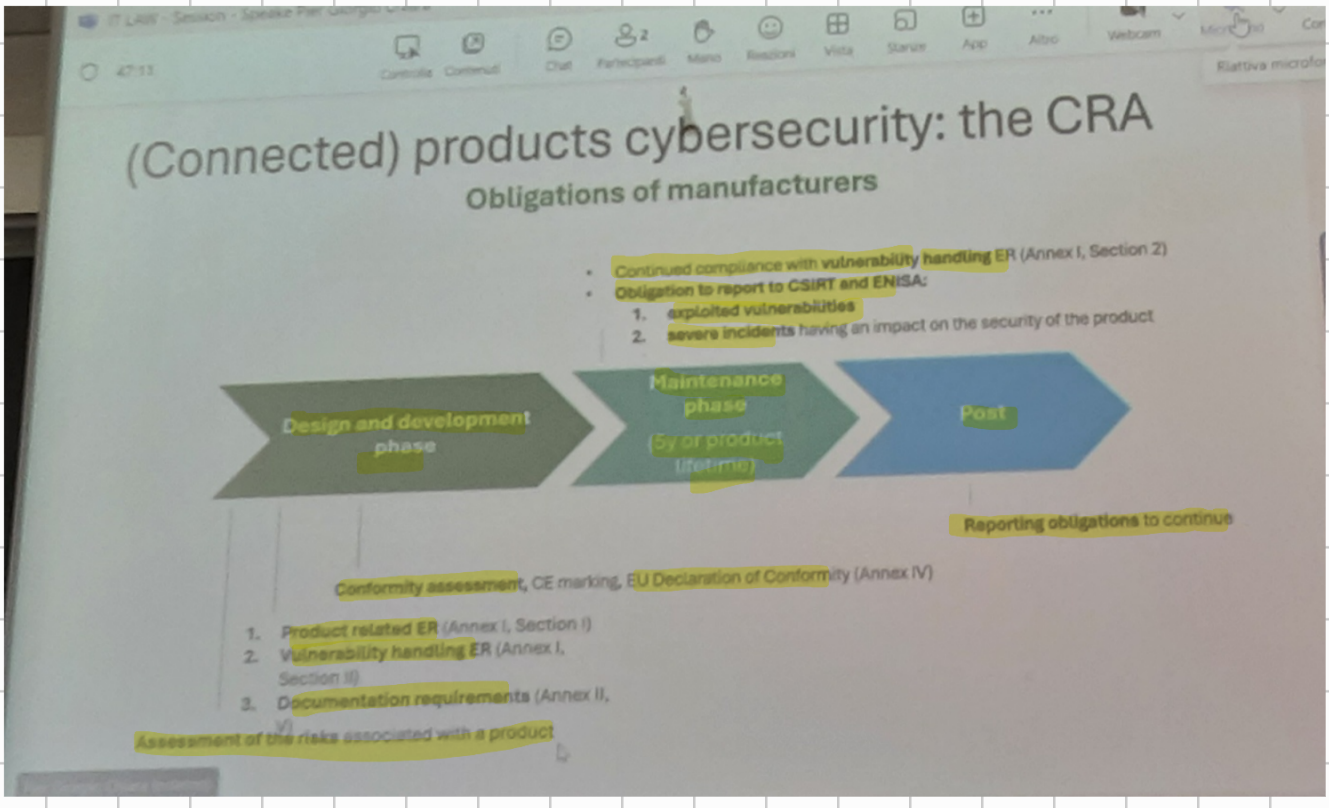
ⓐ We will see to which products this directive applies.



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



* 1 Reg. included in those regulation provide for a sufficient level of protection
Manufacturers will have to comply within 10 years.

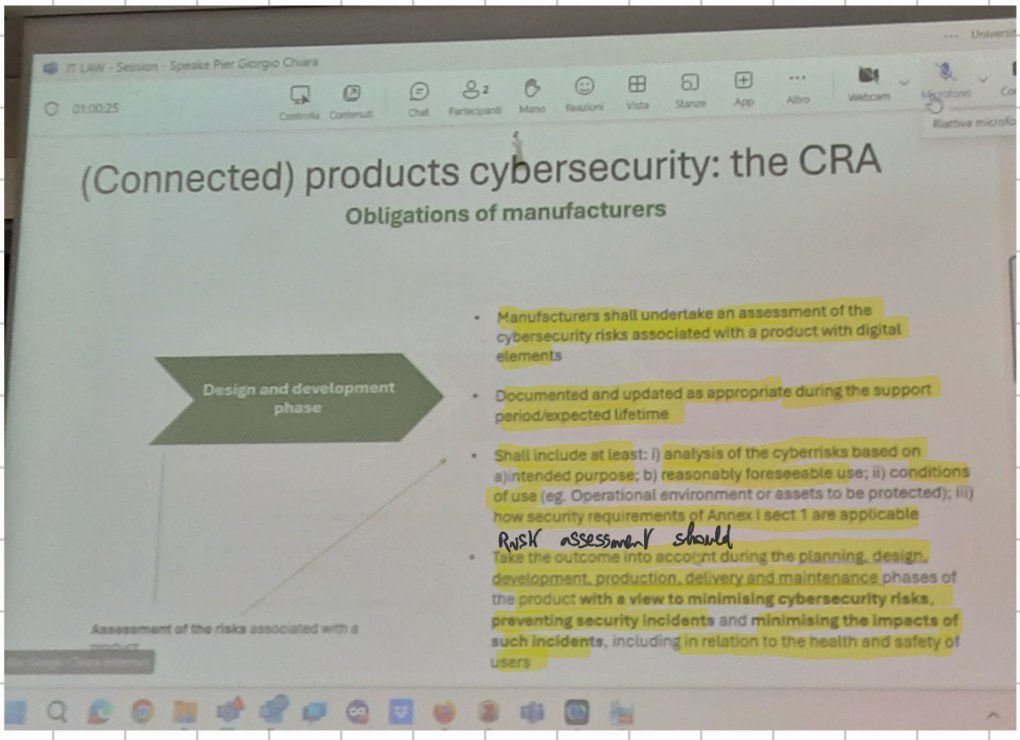


NOTE: The exclusion is there because of other safety or security measure in those sectors. This is done to avoid increasing the burden to producers for additional

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

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

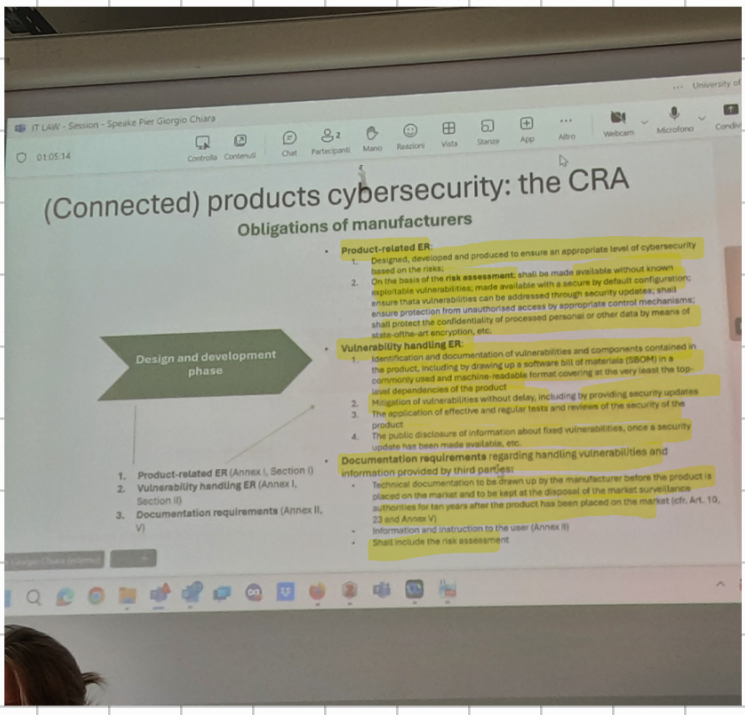
- Everything starts with RISK ASSESSMENT: the Cyber Res. Act, works on a risk based approach.



RISK ASSESSMENT
↓
DOCUMENTATION AND UPDATES DURING THE LIFETIME
↓
RISK ANALYSIS BASED ON INTENDED, FORESEEABLE USE; CONDITION 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.

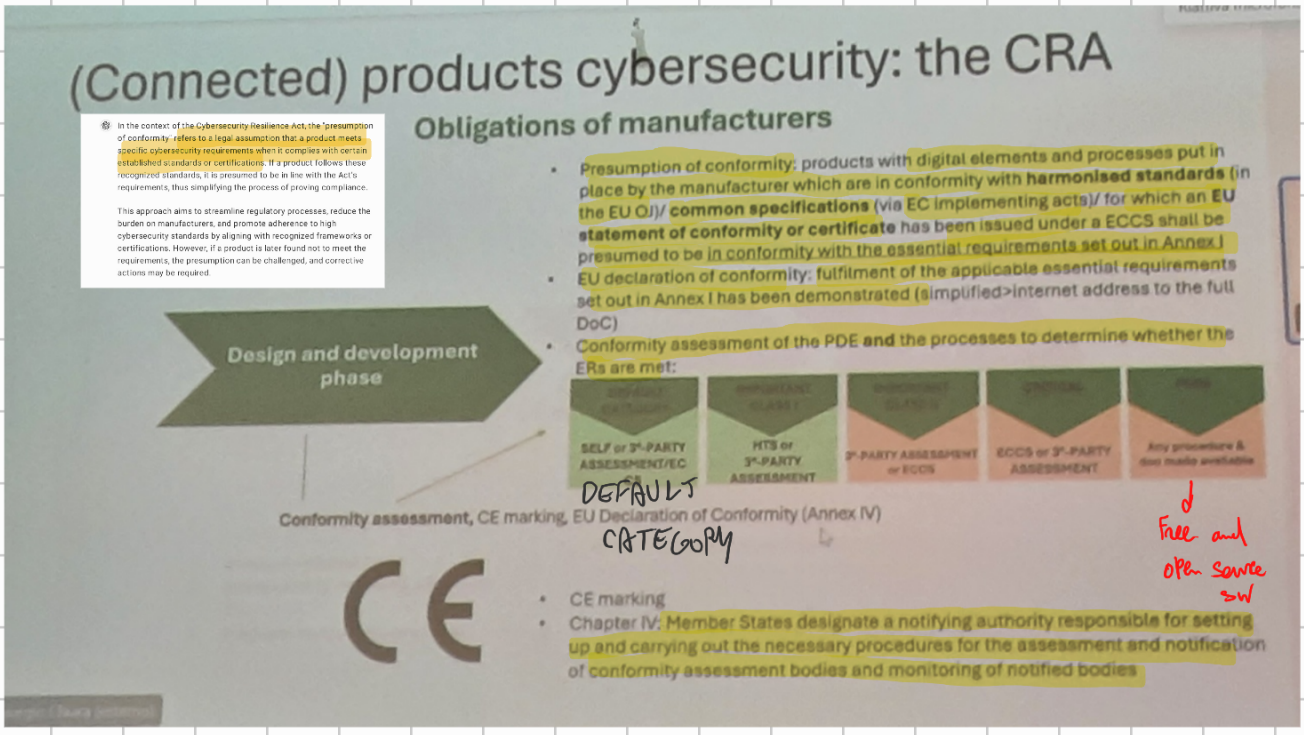
This risk based approach is the overall framework: the first one to shift the approach and put the effort and accountability falls on the provider was GDPR. You are in charge of what are the risks and the measures. It will be up to the manufacturer to prove that they evaluated the risks and took the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



1. ENSURE APPROP. LEVEL OF CS BASED ON RISKS
↳ MAKE PROD. AVAILABLE WITHOUT KNOWN VULN. AND THAT FUTURE VULN. CAN BE ADDRESSED THROUGH SEC. UPDATE AND ENSURE MEASURES FOR CIA
2. MITIGATION OF VULN. WITHOUT DELAY WITH SEC. UPDATES REGULAR TESTS AND REVIEWS OF SECURITY
DISCLOSURE OF INFO ABOUT FIXED VULNERAB. AFTER UPDATE

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

Information that must be disclosed is not confidential in any terms



d Free and open source sw

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.

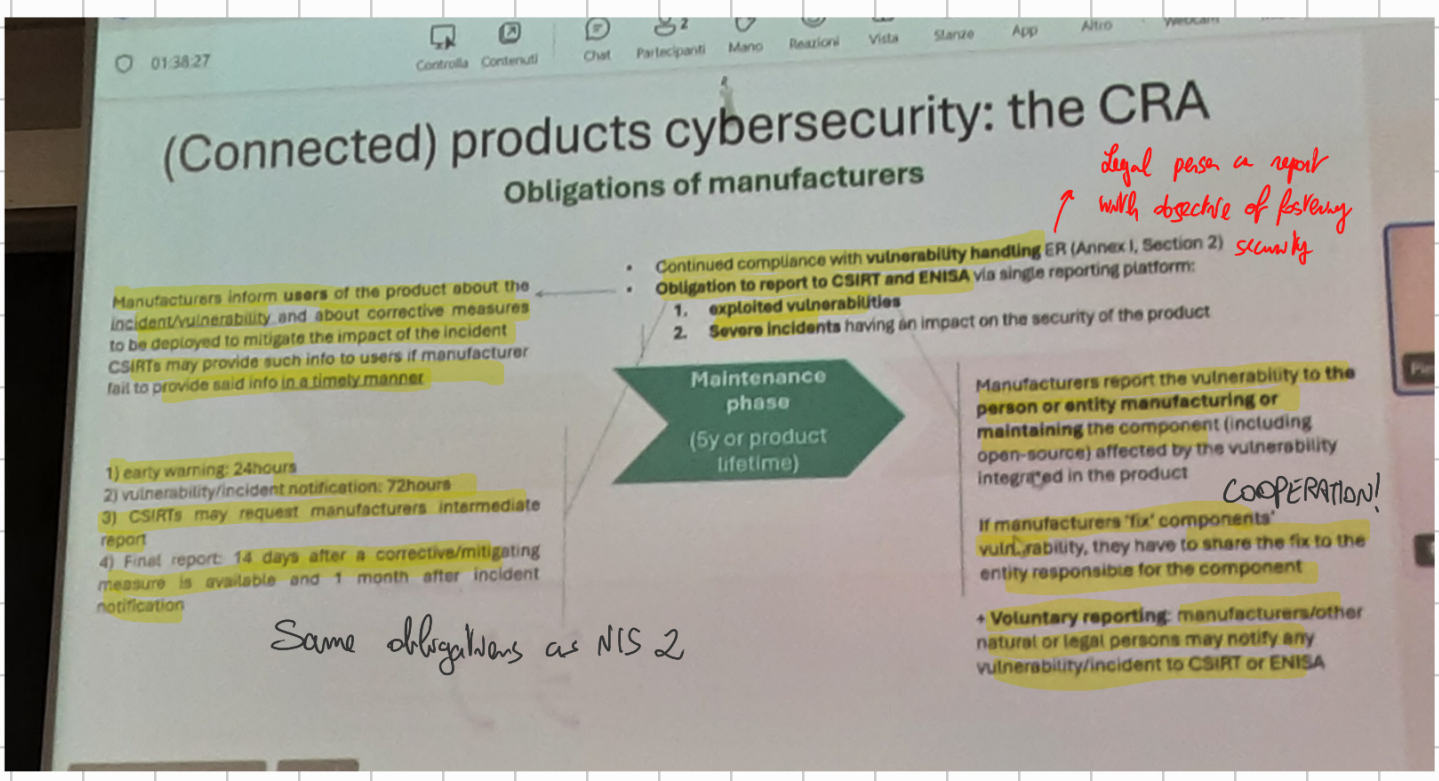
Once a product is presumed to comply the manufacturer can self certify the fullfillment of the Annex I requirement and that the req. have been demonstrated.

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. Certs schemes can emerge, but they require time to be adopted. Not immediately available. "As a commission I will set up basic draft of specifications". Those are a safety net.
Common Criteria can be used to cover 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 important 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 part or EU certs schemes. Critical products present even higher possible risks. There will usually be possible updates on requirements. Skill ECCS if available.
Finally Foss, manufacturers can choose any procedure as long as the docs are made available.

After this manufacturers can apply the CE marking.



Idea vs that vulnerability as a knowledge case: you are aware of a problem. Knowing that it exists as a step forward to the solution of a problem. The vulnerab. might also come from parts of your device: idea vs to ensure the right info sharing chain. Same with vulnerability reporting, goes hand in hand with NIS 2.
The Cyberresilience 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!