CrabNebula

Software as Product

Opportunity and Risk

Daniel Thompson-Yvetot
CEO CrabNebula Ltd.

CRA: From the Regulator

// aims to impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes **direct or indirect data connection** to a device or network.

CRA: From the Regulator

// introduces cybersecurity by design and with default principles and imposes a duty of care for the **lifecycle of products**

CRA: From the Regulator

// As a rule, whoever places on the market a “final” product **or a component** is required to comply with the essential requirements, undergo conformity assessment and affix the CE marking.

CRA: Bird’s Eye View

- Conformity Assessment and CE Marking
- Min. 10 years retention of compliance evidence
- Demonstration of Secure Software Lifecycles
- Incident Response & Market Surveillance
- Alignment with Blue Guide expectations

A quick test…

Does your product have some type of data connection?

Then you will have to comply if you make the product available on the European Market.

Opportunities

Secure by Design
CE Mark as USP
Open Source Stewardship

Secure by Design

Opportunity

Shift-left
Automation
Security as a Service
Policies and Playbooks

CE + Blue Guide

Opportunity

CE Mark as USP

Most software manufacturers will be able to self-certify

Definitions of Manufacturer, Authorised Representative, Importer, Distributor, and End-User do not change.

Open Source Stewardship

Opportunity

Relaxed compliance requirements

No CE Marking, no liability to 3rd Parties

Requires not-for-profit intention

We can help you with such a declaration

Risks

Non-Compliance
Liability to 3rd Parties
3rd Party Obligations to You
Substantial Modifications

Non-Compliance

Risk

Non-compliance can be expensive, potentially reaching up to the higher of €15 million or 2.5% of global turnover. This is not GDPR, it takes time.

Liability to 3rd Parties

Risk

Product integrated by other manufacturers
Potentially includes corporate subsidiaries!

3rd Party Obligations to You

Risk

Others in the Supply Chain might not care
OSS Upstream Dependencies

Substantial Modifications

Risk

Create new products
(Changing the risk profile)
The 5-year compliance clock starts ticking anew

What’s the Timeline?

Enter Into Force (EIF): Expected September 2024
Vulnerability Reporting Obligations: EIF + 21 Months
In Full Application: EIF + 36 Months

How we can help you

Evidence collection and lifecycle retention
Compliance consultation and planning
“Secure by Design” Cybersecurity roadmapping
Serve as your Authorized Representative to the Regulator

CrabNebula