The impact of the CRA on the European ICT sector

19 October 2023

Mirko Boehm
Senior Director, Community Development, Linux Foundation Europe

THE LINUX FOUNDATION | Europe

linuxfoundation.eu

Policy goals supported by most stakeholders

WHAT

- Reduce vulnerabilities in digital products
- Ensure cybersecurity is maintained throughout a product's life cycle
- Enable users to make informed decisions when selecting and operating them

HOW

- "Making products available" defined as "first distribution"
- Obligations regardless of intended or advertised use
- Third-party certification for critical products

€65-95B

... Open source software contributes between €65 to €95 billion to the European Union's GDP and promises significant growth opportunities for the region's digital economy.

EU Cyber Resilience Act - Key Provisions

Everybody who places digital products in the EU market will be responsible for additional obligations around reporting and compliance, such as…

- Fixing discovered vulnerabilities
- Providing software updates across the lifecycle of the products
- Auditing and certifying the products

Responsibilities are born by those who *develop* the software, not downstream users or integrators.

EU Cyber Resilience Act - Coverage

CRA is a horizontal regulation that puts obligations on software manufacturers who publish code that is available in the EU (open source or not, regardless of whether you're in the EU or not).

- **Individual developer of OSS:** "Non-commercial" open source development is excluded. Revenue beyond occasional donations is considered to indicate commercial activity.
- **Nonprofit foundation developing open source:** You will likely need to comply with the CRA requirements. (considered for amendments)
- **Private company** developing, commercializing or supporting open source software: You will very likely be covered under the CRA.

The CRA does not distinguish between open source and closed source software.

EU Cyber Resilience Act - Misconceptions

1. “The developers who know the code best and are best suited to fix vulnerabilities are located upstream”
2. “Open source foundations are large, well-funded fronts for big tech businesses”

Describe, develop and verify a vulnerability fix

Vulnerabilities are reported against a concrete execution context:

- Software
- Hardware environment
- System configuration

In FOSS:

- Downstream use cases are unknown
- Hardware environments are not always available upstream

USGS Bee Inventory and Monitoring Lab, public domain

Implications for EU SMEs and communities

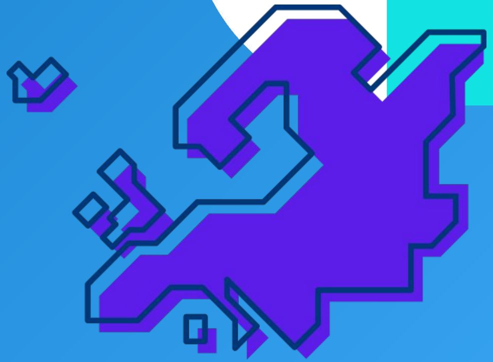
Trust issues: ENISA, member state security registries, other countries?

“Not available in the EU” - only through intermediaries

Regulatory burden - more big tech concentration

EU: CRA compliance from the start
World: CRA compliance on import

The EU Cyber Resilience Act



Does the “Brussels Effect” also work on the open source commons?

We don’t know. We know that the CRA …

- puts additional burdens on SMEs
- disincentivizes upstream-first development
- encourages development offshoring

EU Cyber Resilience Act - How to fix the CRA?

1. Responsibilities and obligations must be aligned with the structure of the supply chain.
2. The commercial entity placing a product on the market must bear the corresponding responsibilities under the CRA.

Thank you!

References:

- Understanding the Cyber Resilience Act: What Everyone involved in Open Source Development Should Know. Ashwin Ramaswami and Mirko Boehm. 08 September 2023
- Will the Cyber Resilience Act help the European ICT sector compete? Mirko Boehm. 12 September 2023