THE RAMIFICATIONS OF THE CRA

Jordan Maris | OSI EU Policy Analyst

What is the CRA?

- **An EU law about the Cybersecurity of products**
  - both physical (Computers, Phones, IoT, routers etc..)
  - and digital (eg: software and software libraries)

- **that also covers the software supply chain:**
  - and impacts how you use dependencies

- **and seeks to make certain Open Source projects more sustainable**
  - by incentivising large downstream users to support development

Who does the CRA impact?

- **Manufacturers of products (you!)**
  - A company that makes a product it monetizes with the intention to make a profit (eg Element)
- **Open Source Software Stewards**
  - An organisation set up to support an Open Source project without the intent to make a profit (eg Mastodon gGmbH)
- **Other Open Source projects**
  - Open Source projects without a Steward, are not subject to the CRA, but do benefit from it in some ways

What do I have to do as a manufacturer?

- **Meet essential cybersecurity requirements**
  - No known vulnerabilities in your product
  - Secure config by default
  - Updatable, preferably automatically
  - Access Control, Encryption of data in transit and where needed at rest, protection of data at rest against unauthorised modification

What do I have to do as a manufacturer?

- **Prepare (technical) documentation**
  - Most important of which: SBOM (Software Bill of Materials)
- **Provide documentation for the user**
  - in particular warning about key risks, and the life/support span of the product
- **Have a vulnerability handling and disclosure policy, and report discovered vulnerabilities within 24 hours.**
- **Provide a EU Declaration of Conformity and affix the CE logo to the software.**

How do I know, and show I comply?

- **To comply with the CRA, your product must undergo a *conformity assessment*.**

	Standard Product	Important Class 1	Important Class 2
Proprietary	Self Assessment	Ext. Assessment	Ext. Assessment
Open Source	Self Assessment	Self Assessment if you publish technical docs	Self Assessment if you publish technical docs

Class 1: Identity/Access Management, Browsers, Password Managers, Antivirus, VPN, Network Management, System Info & Event Management, Boot managers, PKI, Physical & Virtual Network Interfaces, Operating Systems, Routers, Modems, Switches, Microprocessors/controllers/ASIC/FGPA with security functionalities, Smart home virtual assistants,Smart home products with security functionality (door locks), Internet Connected Toys, Health monitoring wearables

Class 2: Hypervisors & Container Runtimes, Firewalls & Intrusion detection and prevention, Tamper resistent microprocessors and controllers.

How do I know, and show I comply?

- There will be *Harmonised Standards* you can follow to show you comply with the law.

- These are currently under development at European Standards Organisations, who are looking for SME's (Small and Medium Entreprises) to provide feedback! Contact me for info

What about Open Source Software Stewards?

- **Lightweight regulatory regime**
  - Comply with vulnerability reporting rules
  - Have Cybersecurity and Vunerability handling Policies
  - Cooperate with authorities with an aim to mitigate risks
  - Look after and handle vulnerability reports for the Open Source project they steward
- **No Fines**
- **Manufacturers can use Open Source projects with a Steward without having to worry about those projects compliance.**

What about Open Source Software Stewards?

- **Lightweight regulatory regime**
  - Comply with vulnerability reporting rules
  - Have Cybersecurity and Vunerability handling Policies
  - Cooperate with authorities with an aim to mitigate risks
  - Look after and handle vulnerability reports for the Open Source project they steward
- **No Fines**
- **Manufacturers can use Open Source projects with a Steward without concerns about compliance.**

What about Open Source Software w/o a steward?

- **Exempt from the law: no obligations**
- **If Manufacturers choose to use it in their product:**
  - They are responsible for ensuring compliance of that code with the CRA.
  - They are **required** to report security flaws to the upstream developer.
  - They are (most likely) **required** to provide any security fix they develop to the original developer

What potential benefits for Open Source companies?

- Less Bureaucracy that proprietary software (Self assessment in lieu of external assessment)
- *Open Source Steward* as a stepping stone between personal project and company
- (TBD): Compliance as a Service: Potential to provide a CE labelled Entreprise edition as a manufacturer, and support a non-CE labelled Community Edition with a software steward.

What is still to be decided?

- Lots of outstanding questions on how exactly the law will apply.
- Eclipse's ORC (Open Regulatory Compliance) WG is working on this.
- Exact approaches to compliance will be set out in Standards (still WIP).

What if I want to get involved/know more?

Read the ORC FAQ

Support work on Standards

Join ORC

Discussion Time!

What if I want to get involved/know more?

Read the ORC FAQ

Support work on Standards

Join ORC