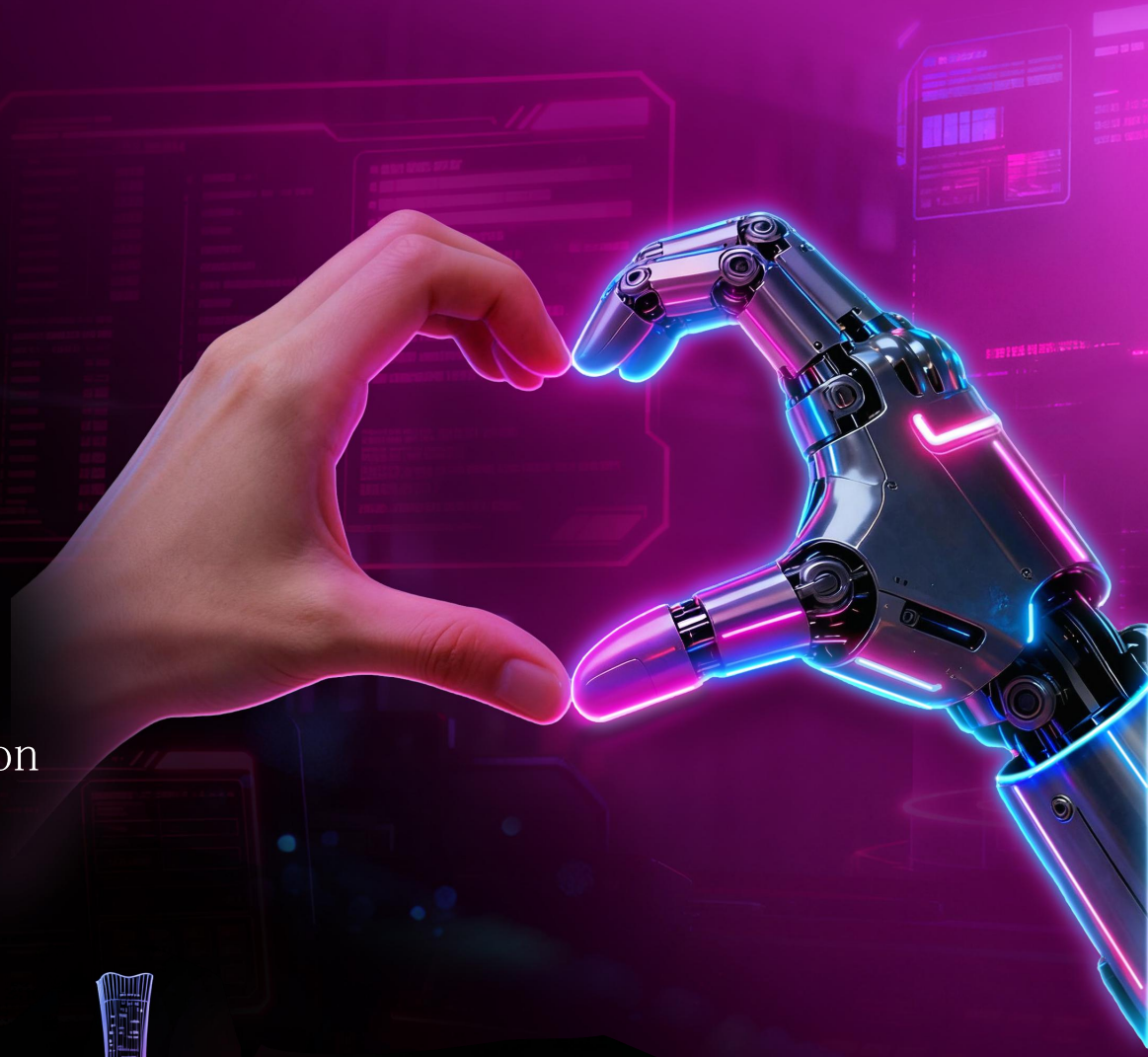
开源社
kaiyuanshe

COSCon'25
第十届中国开源年会

众智开源｜Open Source, Open Intelligence



The Cyber Resilience Act: Practical Steps to Prepare for Europe's Cybersecurity Legislation (SBOMs, Standards and Open Source Software)

Andrew Katz, Bristows LLP and Orcro Ltd

CONTENTS

目录

PART 01 Why the CRA?

Why the CRA?

- The Cyber Resilience Act (CRA) regulates the development, importation and supply of connected products within the EU
- The aim is to reduce cyber risks to EU citizens, businesses and other bodies in the EU
- It is part of a suite of legislation covering product safety for many products including toys, measuring instruments, radio equipment, low voltage electrical equipment, medical devices
- The aim is that *products with digital element* n meet the standard are marked with a CE mark:

CE

Why the CRA?

开源社 kaiyuanshe

- Manufacturers, importers and distributors of PDEs within the European Union are all regulated.
- PDEs are all devices containing software, and standalone software which (in practice) connects or can connect to a network (mainly the internet)
- Penalties are very significant (up to 2.5% worldwide turnover)

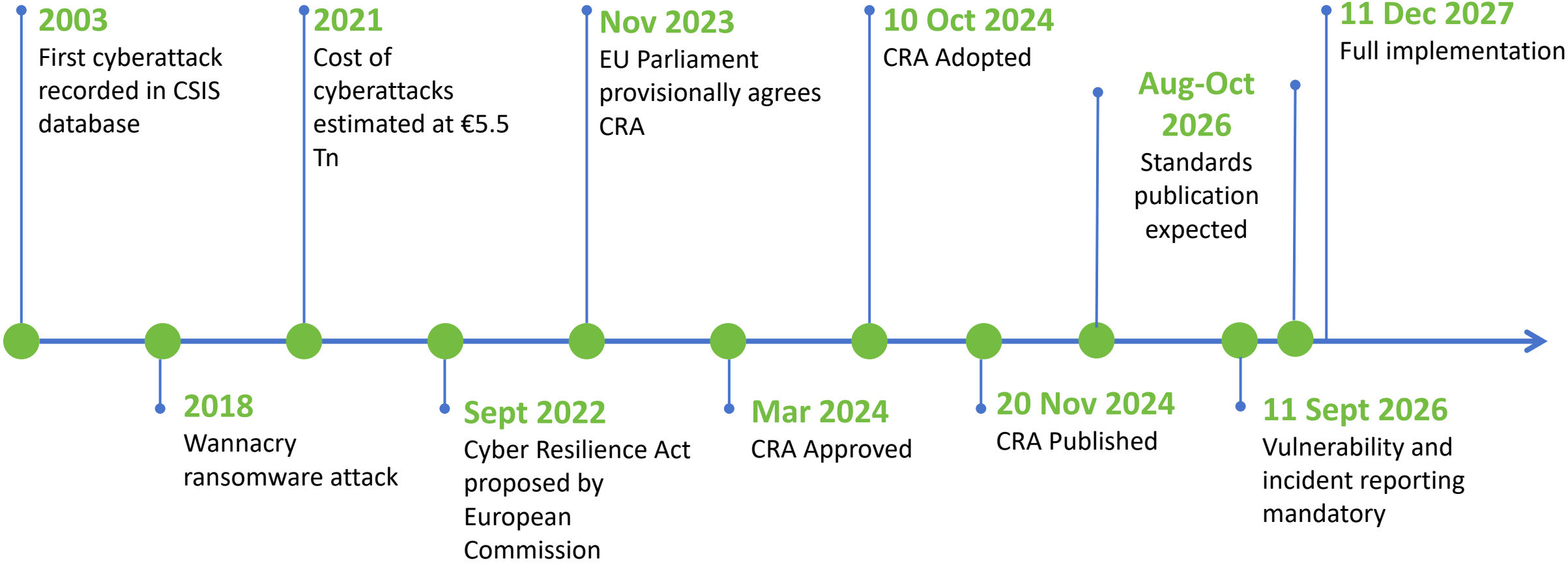
Why the CRA?

开源社 kaiyuanshe

- The CRA sets out:
  - rules for putting any product with digital elements on the market in the EU;
  - essential security requirements on all products during the design, development and lifecycle of the products;
  - vulnerability handling requirements for manufactures for the lifecycle of the product; and
  - market surveillance and enforcement rules.

PART 02 Timeline

Timeline


2003
First cyberattack recorded in CSIS database
2018
Wannacry ransomware attack
2021
Cost of cyberattacks estimated at €5.5 Tn
Sept 2022
Cyber Resilience Act proposed by European Commission
Nov 2023
EU Parliament provisionally agrees CRA
Mar 2024
CRA Approved
10 Oct 2024
CRA Adopted
20 Nov 2024
CRA Published
Aug-Oct 2026
Standards publication expected
11 Sept 2026
Vulnerability and incident reporting mandatory
11 Dec 2027
Full implementation

PART 03 What are your obligations?

Your obligations

开源社 kaiyuanshe

Essential Security Requirements

- **Designed, developed and produced with cybersecurity as a core development principle**
- **Delivered without known exploitable vulnerabilities**
- Delivered with a secure default configuration
- **Ensure vulnerabilities address through security updates**
- **Protection against unauthorised access**
- Protection of confidential data (inc. personal data) by use of encryption etc.
- Maintain integrity of data and protect against corruption and manipulation
- Process only data necessary for intended purpose of the product
- **Resilience against attacks (e.g. DDOS)**
- Implements data minimisation
- Minimises requirements on third party services
- Limits attack surfaces
- Uses appropriate exploitation mitigation mechanisms and techniques
- Records and monitors use etc. to provide security related information
- **Delivers security updates**

Your obligations

开源社 kaiyuanshe

Product Classification

- PDEs are classified into 4 different levels. Different rules apply to different levels
  - For example, manufacturers can self-certify some PDEs
  - Some PDEs will need to be independently assessed for conformity

- Some products are not covered at all (mainly because other regulations already apply to them.
- Standards are being developed covering general requirements (*horizontal*) and specific types of product (*vertical*)
- If a PDE complies with the standard, there is a *presumption of conformity*.

Your obligations

开源社 kaiyuanshe

Vulnerability Handling

- rules for putting any product with digital elements on the market in the EU;
- essential security requirements on all products during the design, development and lifecycle of the products;
- vulnerability handling requirements for manufacturers for the lifecycle of the product; and
- market surveillance and enforcement rules.

PART 04 Practical Requirements?

Practical Requirements

开源社 kaiyuanshe

- Awareness
- Standards
- Tooling
- Supply chain relationships
- Development methodologies
- Risk management

Practical Requirements

开源社 kaiyuanshe

Software Bills of Materials (SBOMs)

- are an important tool in aiding compliance

- Key to information flow up and down the supply chain
- Are not required to be made public
- The European Commission can define the format and elements required in an SBOM
- It must cover “at the very least the top-level dependencies”
- Likely to have to comply with BSI (German) standards
- ENISA has survey which is open until 19th December

Practical Requirements

开源社 kaiyuanshe

- CRA and Open Source
  - Open-source components: select with care
  - Open-source software stewards
  - Individual developers
- “Open-source software stewards”
  - E.g. Eclipse Foundation, Linux Foundation
  - Must implement a Cybersecurity Policy
    - To foster the development of secure products
    - To foster the development of effective vulnerability handling and reporting
    - Sharing information and co-operate with market surveillance authorities
  - OSS Stewards are **not** subject to financial penalties

Practical Requirements

- Supply chain information and liability flow
- Familiarise yourself with
  - SPDX 3.0 (CycloneDX)
  - OpenSSF Scorecard
  - OpenChain
- Preparing your suppliers: map your supply chain
- Supplier due diligence (e.g. OpenSSF Scorecard)
- Supply contracts:
  - Development framework: methodologies for developing secure code
  - Security by design: set design parameters
  - Open development process
  - Dataflow: how to manage, address vulnerabilities
  - SBOM standards used, and testing
  - Ongoing vulnerability reporting framework for lifecycle of the product

Practical Requirements

- Classify risks
  - Classify suppliers:
    - commercial (paid);
    - commercial (OSS);
    - OSS Stewards
    - non-stewarded
- Triage software
  - Build into your code selection policy
  - Where in the stack is it (how likely is it to present a vulnerability)?
  - Is the technology/framework/language inherently more secure (e.g. Rust)
  - Code-selection: look at how well the project handles vulnerabilities

Practical Requirements

- Manage Risks
  - Pooling information: establish information pools?
    - Industry-based
    - Vertical-market based
    - Product based
    - Foundations/OSS Stewards
  - Outsourcing vulnerability management? (Cannot outsource *responsibility*).
  - Establish incident response protocols. Co-ordinate

Practical Requirements

- Record Keeping
  - Record design principles for the PDE (security by design)
  - Retain SBOMs for all releases
    - Identify source of SBOMs (internally generated? Generated by suppliers?)
  - Record component selection
  - Record vulnerability testing protocols
- Record incidents and responses
  - Responses include fixes: requirement to pass back to supplier/to the original project?
- Leverage SPDX for risk management?
  - CRA profile

Practical Requirements

What is happening?

- Standards are continuing to be developed
  - Directly mandated (CEN-CENELEC/ETSI), Release in 2026
  - Further related standards being developed (e.g. BSI, SPDX. OpenChain)
- Industry and the European Commission are engaging with each other through regular meetings and fora
- Industry bodies (companies, OSS foundations etc) are collaborating on industry approaches
- Data-sharing likely to occur at
  - Project level
  - Through OSS Foundations
  - Through national/international initiatives (e.g. ENISA, NCSC, NSA)

Practical Requirements

开源社 kaiyuanshe

Example projects (Linux Foundation research)

- Yocto Project (toolkit for creating embedded Linux systems)
  - Classifies itself as an “open-source software steward”
  - Conducts cybersecurity risk assessments through CVE monitoring and implements build-time CVE
  - Currently releases 4-year LTS version. May extend to 5 years (CRA)
  - Reproducible builds (arguably goes beyond CRA requirements)
- Zephyr Project (realtime operating system project)
  - Classifies itself as an “open-source software steward”
  - Git-based development and releases
  - 2.5 year support window (<5 year CRA requirement)
  - CVE Numbering Authority Status
  - Uses OpenSSF Scorecard

Practical Requirements

开源社 kaiyuanshe

Linux Foundation Recommendations

- Build a sustainable security roadmap
- Align development practices to CRA
- Invest in tooling for compliance and security
- Standards development and cross-sector collaboration
- Address emerging security challenges
- Effective, empowered and resourced leadership for open source software security

Updates (as of 3rd December)

New European Commission site: https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

FAQ Document:

https://ec.europa.eu/newsroom/dae/redirection/document/122331

- Clarity on relationship between CRA and PLD (Product Liability Directive), GPSR (General Product Safety Regulation), GDPR and others
- Clarity on combining elements with different risk levels/criticality
- Clarity on carrying out risk assessments (and intended purpose and reasonably foreseeable use)
- Products need not be vulnerability free: covers known exploitable vulnerabilities based on risk assessment
- In extreme cases, a recall may be required
- If a component is CE marked, the manufacturer can rely on the associated declaration of conformity.
- For stewarded OSS, the commission may establish voluntary attestation programmes (see https://github.com/orcwg/cra-attestations)
- Criteria for support period
- Reporting Obligations
- Conformity assessments
- Transition

Further sources of information:

开源社 kaiyuanshe

- Open Regulatory Compliance Working Group: https://orcwg.org/
- OpenChain: https://openchainproject.org/
- SPDX: https://spdx.dev/
- OpenSSF Scorecard: https://openssf.org/projects/scorecard/
- CEN/CENELEC: https://www.cencenelec.eu/
- European Commission CRA: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- ENISA: https://www.enisa.europa.eu/
- Support for micro-, small- and medium-sized enterprises: https://digital-strategy.ec.europa.eu/en/policies/cra-msmes
- CRA Expert Group: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967

EU Recommended Sources of information

开源社 kaiyuanshe

OCCTET - ‘Open-source Compliance: Comprehensive Techniques and Essential Tools’ https://occtet.eu/

CONFIRMATE - ‘Conformity assessment, metrics and compliance automation for the Cyber Resilience Act’ https://confirmate-project.eu/

CRACY - ‘CRA made Easy’ https://cra-cy.eu/

CYBERFORT - ‘Strengthening Cyber Defenses of SMEs for CRA Compliance’ https://cyber-fort.eu/

CURIUM - ‘Transformation into a Trustworthy Certified Digital Valley’ https://curium-project.eu/

OSCRAT - ‘Open-Source Cyber Resilience Act Tools’ https://oscrat.eu/

CRA-AI - ‘A European collaboration to drive CRA conformity for SMEs using AI Innovation’ https://www.cybercertlabs.com/cra-ai/

SECURE - ‘Strengthening EU SMEs Cyber Resilience’ https://secure4sme.eu/

STAN4CR - ‘Standardization in support of the EU Cyber Resilience Act’ https://www.stan4cra.eu/

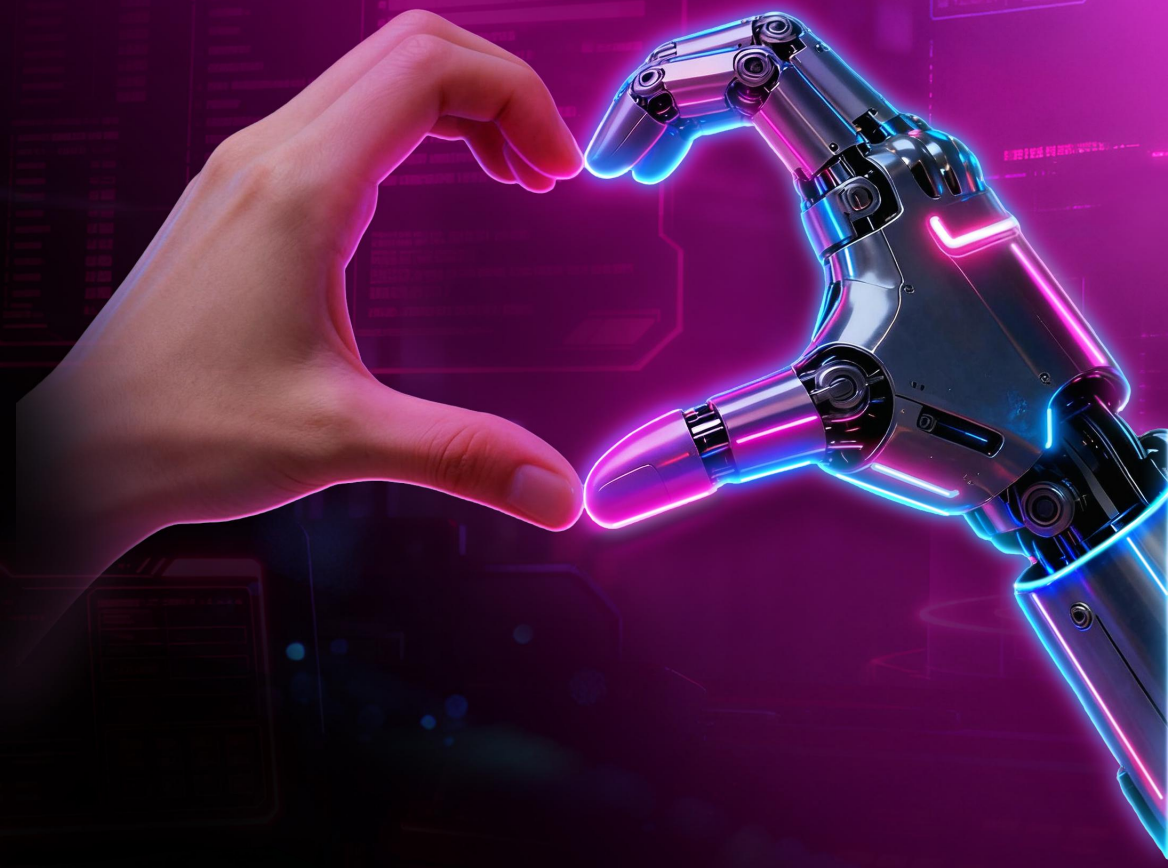
CYBERSTAND - ‘Supporting EU experts in Cybersecurity standardisation activities’ https://cyberstand.eu/

开源社
kaiyuanshe

COSCon'25
第十届中国开源年会

众智开源｜Open Source, Open Intelligence

Thanks



Andrew Katz

andrew.katz@bristows.com
andrew.katz@orcro.co.uk