RSAC 2026 Conference

POWER OF COMMUNITY.

SESSION ID: PART3-W09

The EU Cyber Resilience Act — What's in it for Industry?

Prof. Dr. Norbert Pohlmann

Director **Institut for Internet Security** - if(is),
Gelsenkirchen, Germany
President, **TeleTrusT,** Berlin, Germany
https://www.linkedin.com/in/norbert-pohlmann-a2b9775/

Nevena Rupp

Director-General of Digitization and Identities
Federal Office for Information Security (BSI)
Bonn, Germany
https://www.linkedin.com/in/nevenarupp

RSAC 2026 Conference

©peterschreiber.media / stock.adobe.com

Cyber Resilience Act

Motivation

Framework

Guidance

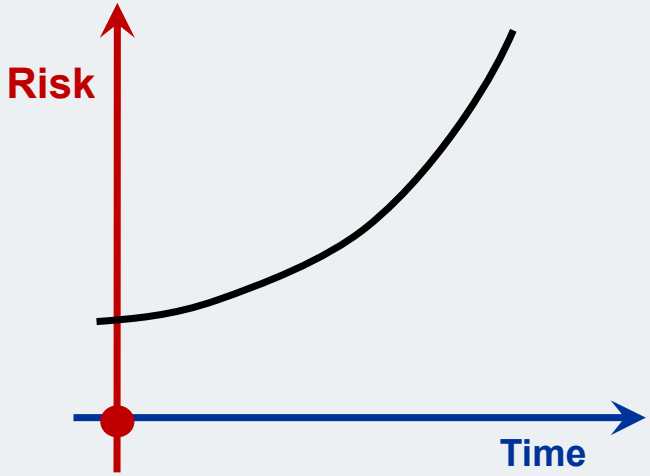
Summary

POWER OF COMMUNITY.

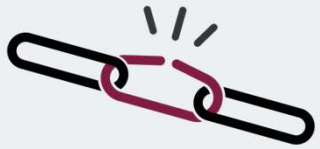
Let’s start with a simple truth

The current cybersecurity situation

- IT risks are becoming increasingly complex and difficult to manage.



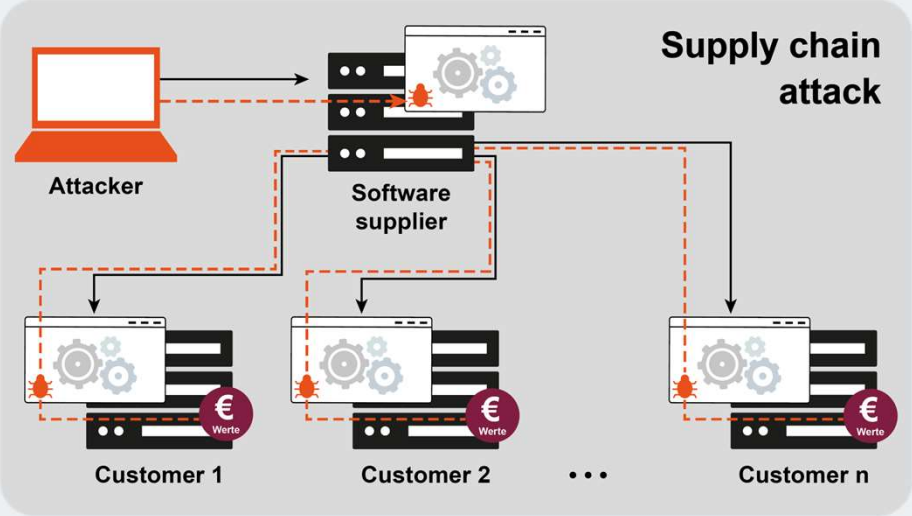
- IT systems are not “secure by design”.



Why software is the core challenge?

- **Software** is the **central risk driver** in today's digital world.
- The IT systems are and the software is becoming: More **complex**, more **interconnected**, faster **developed** and increasingly **AI-driven**.

- **IT Supply Chain Security**



What can be done?

- Technically, the software industry is fully capable of developing more **secure products** and **more resilient update processes**.
- However, **market forces** alone are **insufficient**.

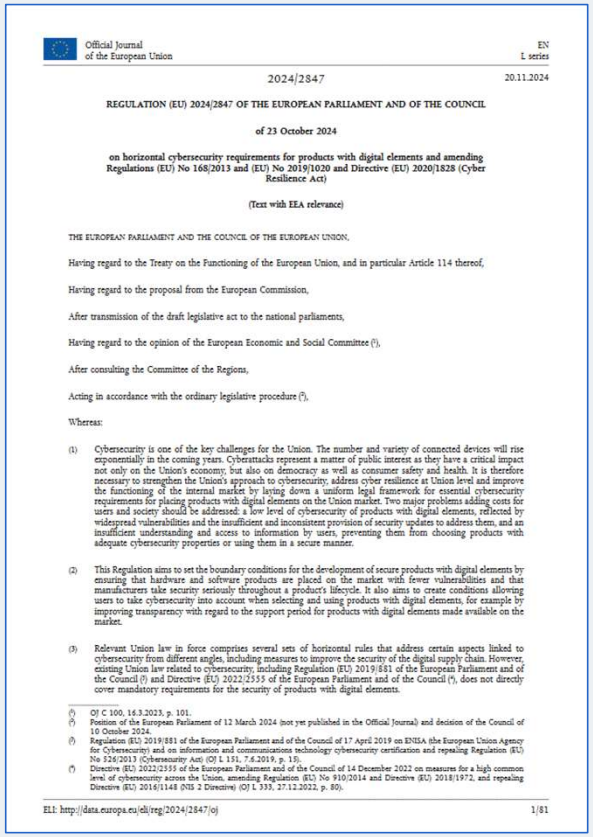
- What can policymakers do?
- **They can establish binding requirements.**
- And that is exactly the purpose of the Cyber Resilience Act.
- The CRA is not designed to burden industry.
- It is designed to **restore trust** and **create a reliable framework** for **secure digital products**.

Why is the CRA so important?

Cyber Resilience Act (CRA)

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

- Establishes **binding**, **uniform cybersecurity requirements** for all digital products.
- It addresses a structural problem: many **IT products** on the market today **have known vulnerabilities**, with **no clear responsibilities** for security and updates.



Official Journal of the European Union — EN, L series

2024/2847 — 20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements, for example by improving transparency with regard to the support period for products with digital elements made available on the market.

(3) Relevant Union law in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, existing Union law related to cybersecurity, including Regulation (EU) 2019/881 of the European Parliament and of the Council (3) and Directive (EU) 2022/2555 of the European Parliament and of the Council (4), does not directly cover mandatory requirements for the security of products with digital elements.

(1) OJ C 100, 16.3.2023, p. 101.
(2) Position of the European Parliament of 12 March 2024 (not yet published in the Official Journal) and decision of the Council of 10 October 2024.
(3) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).
(4) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

ELI: http://data.europa.eu/eli/reg/2024/2847/oj — 1/81

http://data.europa.eu/eli/reg/2024/2847/oj

Clear accountability

- Manufacturers and vendors are explicitly responsible for:
  - **Secure design** and **development**
  - **Systematic vulnerability handling** and **coordinated disclosure**
  - **Timely security updates** throughout the product lifecycle

Raising the baseline security level

- Modern **cyber risks** are **systemic** - especially through supply chains.

- The Cyber Resilience Act addresses this by requiring:
  - **Risk management** for **third-party components**
  - **Transparency about software dependencies** - for example through Software Bills of Materials (SBOMs)
  - **Consistent vulnerability management** across the supply chain

RSAC 2026 Conference

©peterschreiber.media / stock.adobe.com

Cyber Resilience Act

Motivation

Framework

Guidance

Summary

POWER OF COMMUNITY.

Cyber Resilience Act: Main objectives

- Create conditions for the **development of secure products** with digital elements by ensuring that
  - Hardware and software products are **placed on the market with fewer vulnerabilities**
  - **Security throughout life cycle**
- Enable **users to factor in cybersecurity** when buying products with digital elements
- Form **EU wide requirements**, prevent of national fragmentation

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Cyber Resilience Act: Specific Focus

- Ensure that manufacturers **improve the security** of products with digital elements from the design and development phase and **throughout the whole life cycle**
- Ensure a **coherent cybersecurity framework**, facilitating compliance for hardware and software manufacturers
- Enhance the **transparency of security properties** of products with digital elements
- Enable businesses and consumers to **use products with digital elements securely**

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

CRA-Framework: Essential requirements (1/4)

Security requirements relating to the properties of products with digital elements

- Security-by-design, Security-by-default
- protection from unauthorised access; protection of confidentiality and integrity of data
- designed, developed and produced to limit attack surfaces […]

Vulnerability management

- SBOM at the very least of the top-level dependencies of the product;
- Address and remediate vulnerabilities without delay, including by providing security updates
- Public disclosure of information about fixed vulnerabilities, information allowing users to identify the product […]

Minimum information for the user

- Contact information where cybersecurity vulnerabilities of the product can be reported and received
- Identification of product, intended use
- Possibility to assess conformity information and if made available SBOM […]

CRA-Framework: Essential requirements (2/4)

Security requirements relating to the properties of products with digital elements

- Security-by-design, Security-by-default
- protection from unauthorized access; protection of confidentiality and integrity of data
- designed, developed and produced to limit attack surfaces […]

CRA-Framework: Essential requirements (3/4)

Vulnerability management

- SBOM at the very least of the top-level dependencies of the product;
- Address and remediate vulnerabilities without delay, including by providing security updates
- Public disclosure of information about fixed vulnerabilities, information allowing users to identify the product […]

CRA-Framework: Essential requirements (4/4)

Minimum information for the user

- Contact information where cybersecurity vulnerabilities of the product can be reported and received
- Identification of product, intended use
- Possibility to assess conformity information and if made available SBOM […]

Market surveillance ensures compliance

Tools for checks by market surveillance authorities

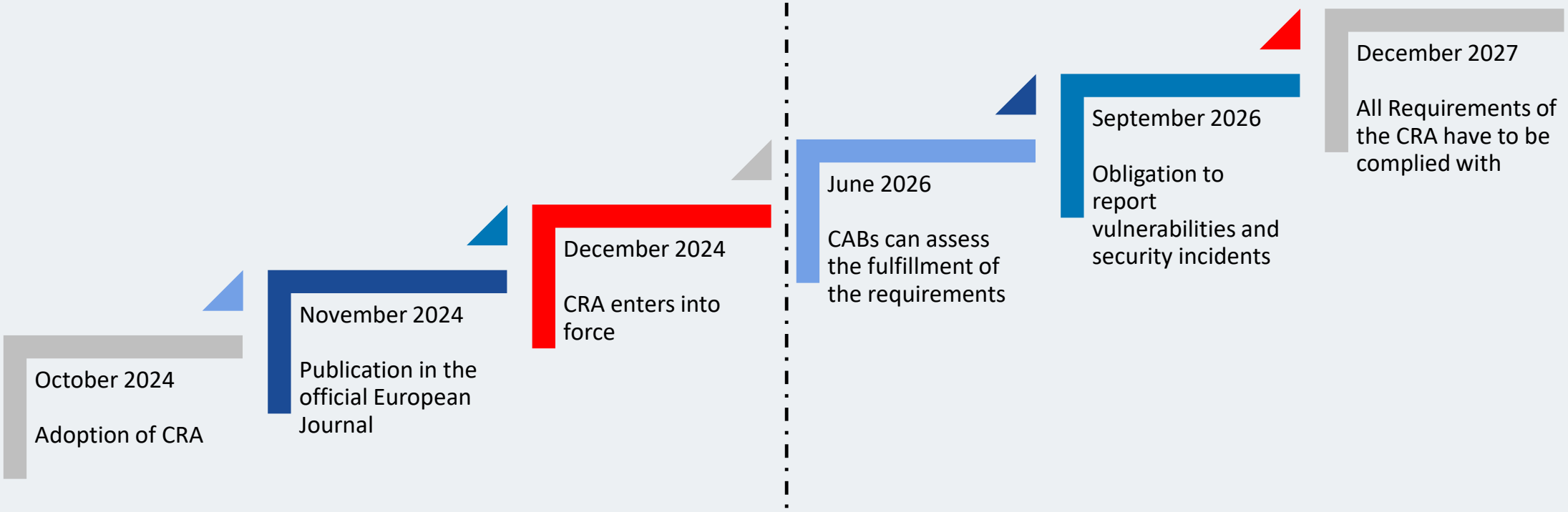
- Documentary checks
- Requests for information
- Inspections
- Laboratory checks
- …

In case of identified non-compliance, market surveillance authorities have powers to:

- require manufacturers to **mitigate non-compliance** and eliminate risk
- to **prohibit/restrict the making available of a product** or to order the product to be **withdrawn/recalled**
- impose **penalties** (including fines up to 15 000 000 EUR or up to 2.5 % of worldwide turnover).

Timeline of CRA

September 2026 is the first externally measurable milestone for vendors: failing to report security incidents and flaws is in violation of CRA.



RSAC 2026 Conference

©peterschreiber.media / stock.adobe.com

Cyber Resilience Act

Motivation

Framework

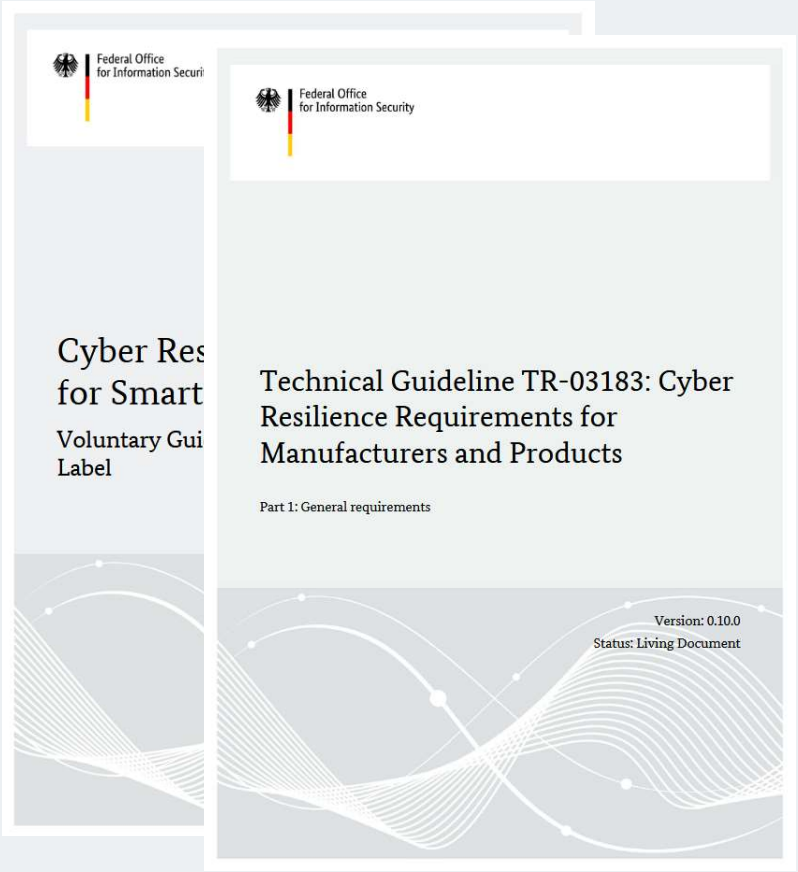
Guidance

Summary

POWER OF COMMUNITY.

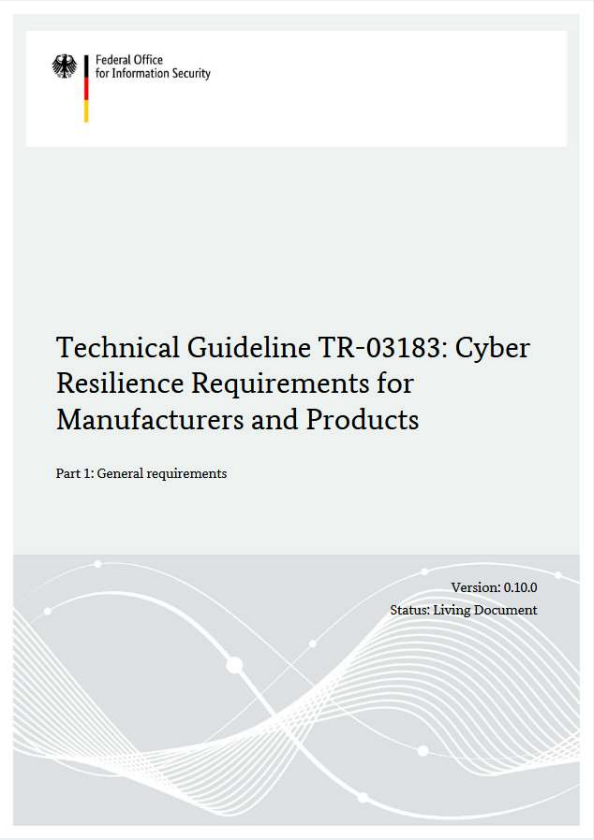
BSI guidance & support

- BSI TR-03183
  Cyber Resilience Requirements for Manufactures and Products
- (federal) IT Security Label
- Website with guidance, information documents, FAQs and links
- https://www.bsi.bund.de/dok/cra-en



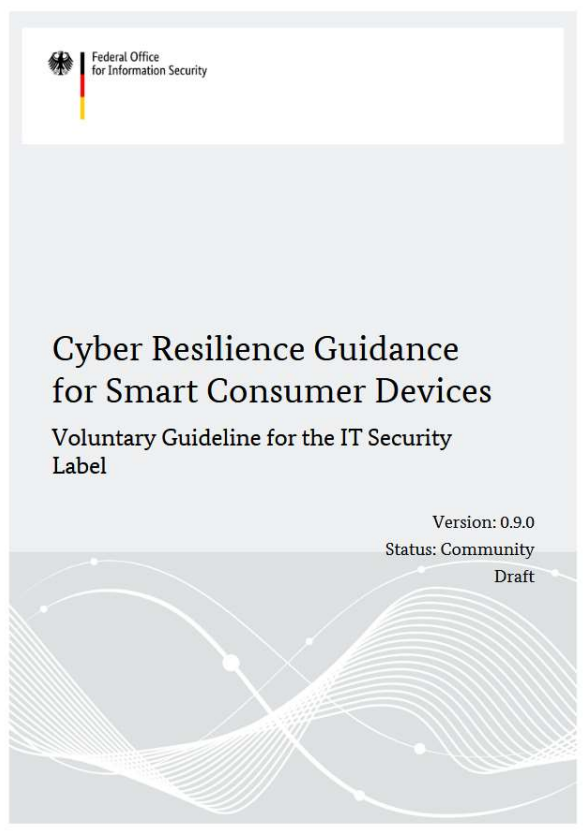
BSI guidance & support
Technical Guideline BSI TR-03183

- describes the **BSI interpretation** of the Cyber Resilience Requirements for Manufacturers and Products and serves to prepare for requirements of the Cyber Resilience Act (CRA).
- is intended as a **collection of information** and as an **introductory guide to the CRA**, particularly for manufacturers who have not yet established mature IT security processes as part of their development and vulnerability handling.
- is meant to be **a guide** and is not binding or mandatory. It cannot be used as presumption of conformity.
- will be gradually **developed further** and replaced by the corresponding harmonized European standards as soon as they become available.



BSI guidance & support
IT Security Label

- Prepare for the Cyber Resilience Act (CRA) with the (federal) **IT Security Label**
- prepares for the mandatory regulation of the CRA
- cybersecurity of products as **selling point.**
- existing requirements of the IT Security Label will **gradually align with the security objectives of the CRA**, allowing manufacturers to integrate them early into their product development.
- product category “Smart Consumer Devices” - which includes most IoT and smart home products – has already a **product-specific supplementary document**



RSAC 2026 Conference

©peterschreiber.media / stock.adobe.com

Cyber Resilience Act

Motivation

Framework

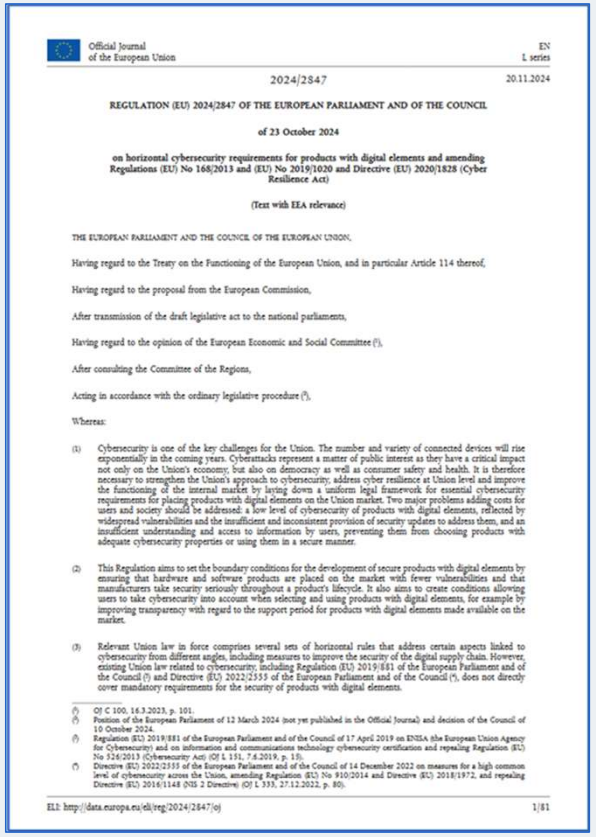
Guidance

Summary

POWER OF COMMUNITY.

Cyber Resilience Act Summary

- CRA regulates the **market access** in form of **horizontal European cybersecurity requirements** for a broad range of **digital products and services**
- Includes requirements for products across the **whole life cycle**
- **Protects** against „fire and forget“ products and **values quality** vendors
- Enables interested **parties to participate in standardization** of requirements



Official Journal of the European Union — EN — L series

2024/2847 — 20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

(2) This Regulation aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements, for example by improving transparency with regard to the support period for products with digital elements made available on the market.

(3) Relevant Union law in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, existing Union law related to cybersecurity, including Regulation (EU) 2019/881 of the European Parliament and of the Council (3) and Directive (EU) 2022/2555 of the European Parliament and of the Council (4), does not directly cover mandatory requirements for the security of products with digital elements.

(1) OJ C 100, 16.3.2023, p. 101.
(2) Position of the European Parliament of 12 March 2024 (not yet published in the Official Journal) and decision of the Council of 10 October 2024.
(3) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).
(4) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

ELI: http://data.europa.eu/eli/reg/2024/2847/oj — 1/81

http://data.europa.eu/eli/reg/2024/2847/oj

Thank you for your attention!

Questions?

Apply what you learned

- **Recognize the growing complexity** of digital products with their Software and **look** for them in your company.
- **Take immediate action** in your company to protect yourself from the increasing risks.
- **Implement clear responsibility** for high-quality software and prompt updates.

Visit the German Pavilion at North Expo Hall, Booth 5469

#RSAC

The Partners at the German Pavilion at RSAC Conference 2026

AWARE7

KOBIL

LocateRisk
MEASURE · COMPARE · OPTIMIZE IT SECURITY

MTRIX® GmbH
[AUTHENTICATION SOLUTIONS]

NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

ONEKEY

SerNet

TÜV SÜD

TÜVIT
TÜVNORDGROUP

unosecur

TeleTrusT
Pioneers in IT security.
IT Security Association Germany

TeleTrusT
Pioneers in IT security.
IT Security Association Germany

Federal Office
for Information Security

RSAC 2026 Conference

RSAC | 2026 Conference

Thank you

POWER OF COMMUNITY.