ETSI Security Conference 2022

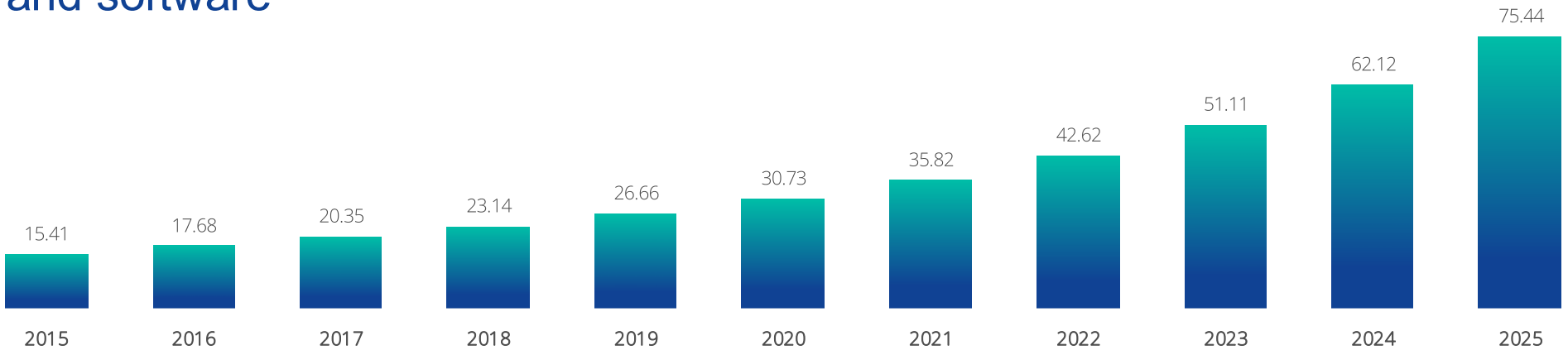
The Cyber Resilience Act

Maika Fohrenbach, DG CONNECT, European Commission

03/10/2022

Everything is connected

- Large majority of vulnerabilities exploitable **over the Internet**
- **Impact assessment: no incentives** to produce secure by design hardware and software



Internet of Things devices worldwide from 2015 to 2025 (in billions)

Source: Forbes/IHS

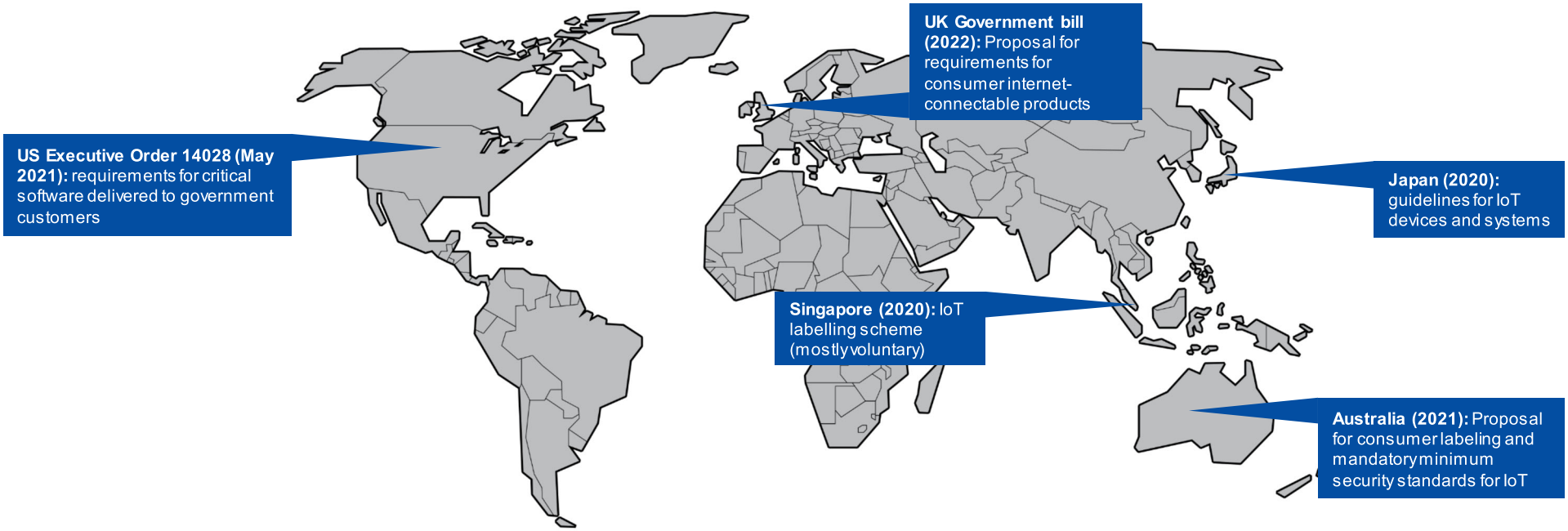
European Commission

Impact of security incidents

- Average cost of a data breach for individual businesses was **EUR 3.5 million in 2018**.
- Statistically speaking, **every 11 seconds** another organisation is hit by a ransomware attack.
- In 2021 alone cybercriminals were able to leverage hacked devices and **launch 9.75 million DDoS attacks** worldwide.
- **57% of SMEs** say they would go out of business in the event of a cybersecurity attack.
- The aggregate cost of security incidents affecting businesses in Germany amounts to **EUR 220 billion in 2020**.

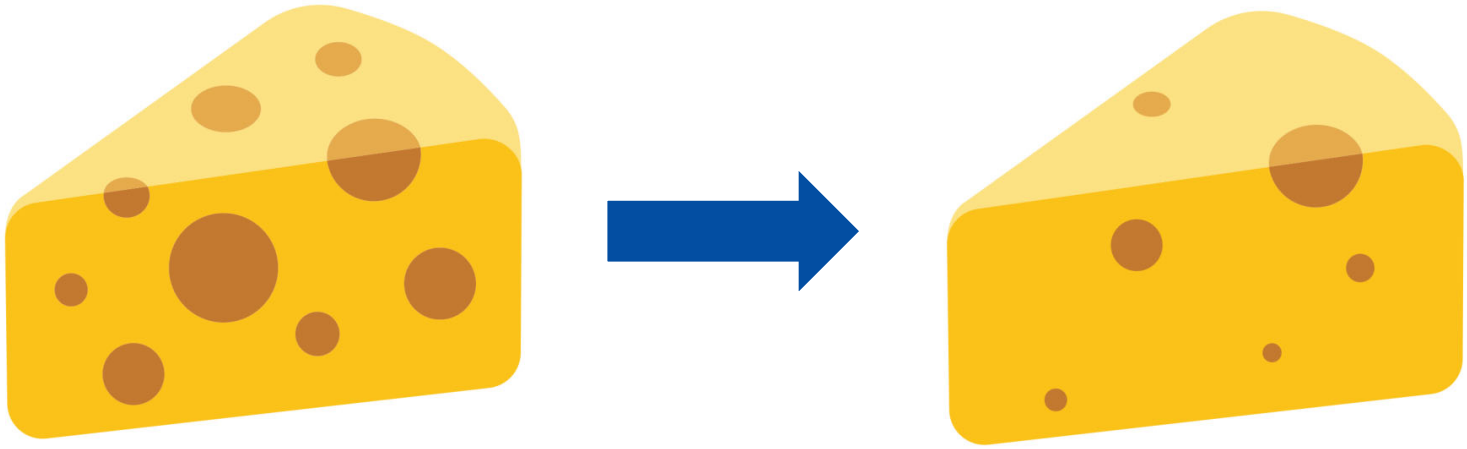
Sources: Ponemon Institute, Cybersecurity Ventures, Netscout, ENISA, Bitkom

Third-country initiatives



European Commission

CRA in a nutshell



European Commission

Main elements of the proposal

- **Cybersecurity rules** for the placing on the market of hardware and software
- Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle (5 years)
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**

European Commission

Scope

Products with digital elements:

- ✚ **Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- ✚ **Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- ⓘ The definition of **"products with digital elements"** also includes **remote data processing solutions.**

Not covered:

- ✖ **Non-commercial projects, including open source** in so far as a project is not part of a commercial activity
- ✖ **Services, in particular cloud/Software-as-a-Service** – *covered by NIS2*

Outright exclusions:

- ✖ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

European Commission

Obligations of manufacturers

Assessment of the risks associated with a product

(1) Product-related essential requirements (Annex I, Section 1)
(2) Vulnerability handling essential requirements (Annex 1, Section 2)
(3) Technical file, including information and instructions for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

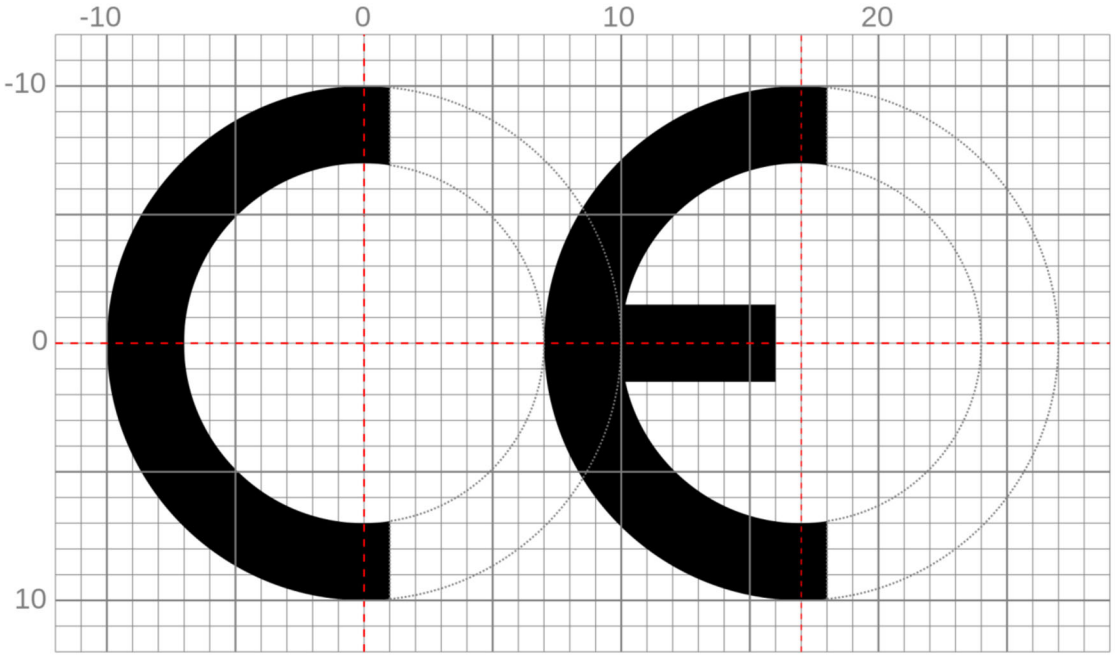
Obligation to report to ENISA within 24 hours:

(1) exploited vulnerabilities
(2) incidents having an impact on the security of the product

Reporting obligations to continue

European Commission

CE marking

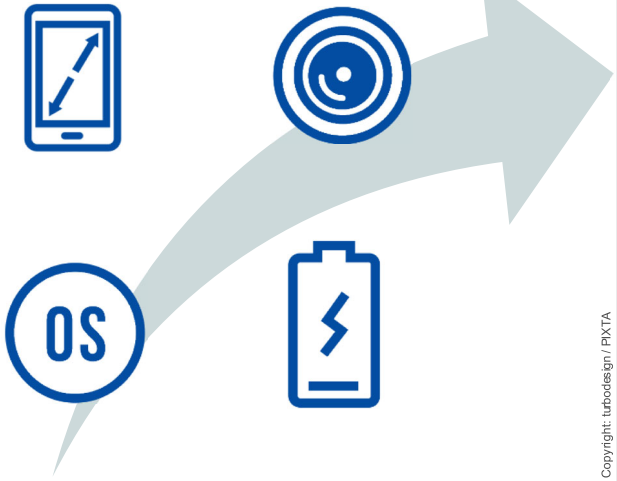


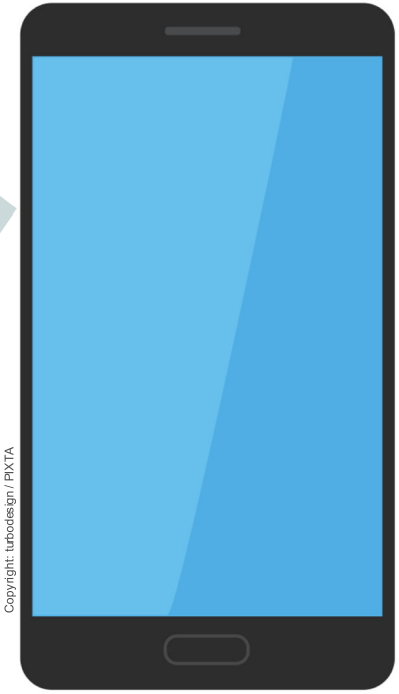
European Commission

A simplified example of smartphones

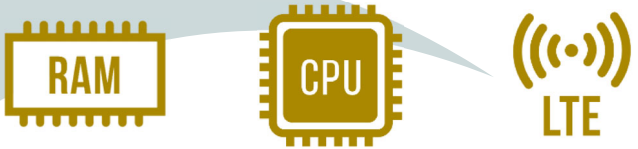
*As a rule, whoever places on the market a **"final" product or a component** is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking.***

Developed by the manufacturer placing the smartphone on the market:





Developed by upstream manufacturers for integration into the "final" product:



Placed on the market separately for users to buy and integrate:

European Commission

Which conformity assessment to follow?

90% of products	10% of products		
Default category	**Critical "Class I"**	**Critical "Class II"**	**Highly critical**
Self-assessment	**Application of a standard or third party assessment**	**Third party assessment**	**Mandatory EU certification**
Criteria: **n/a**	**Criteria:** • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact)		**Additional criteria:** • Used by **NIS2** entities • Resilience of **supply chain**
	To be amended/specified via delegated acts		
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	**Examples (Annex III):** Password managers, network interfaces, firewalls, microcontrollers etc.	**Examples (Annex III):** Operating systems, industrial firewalls, CPUs, secure elements etc.	**Examples:** **n/a** (empowerment to future-proof the CRA)

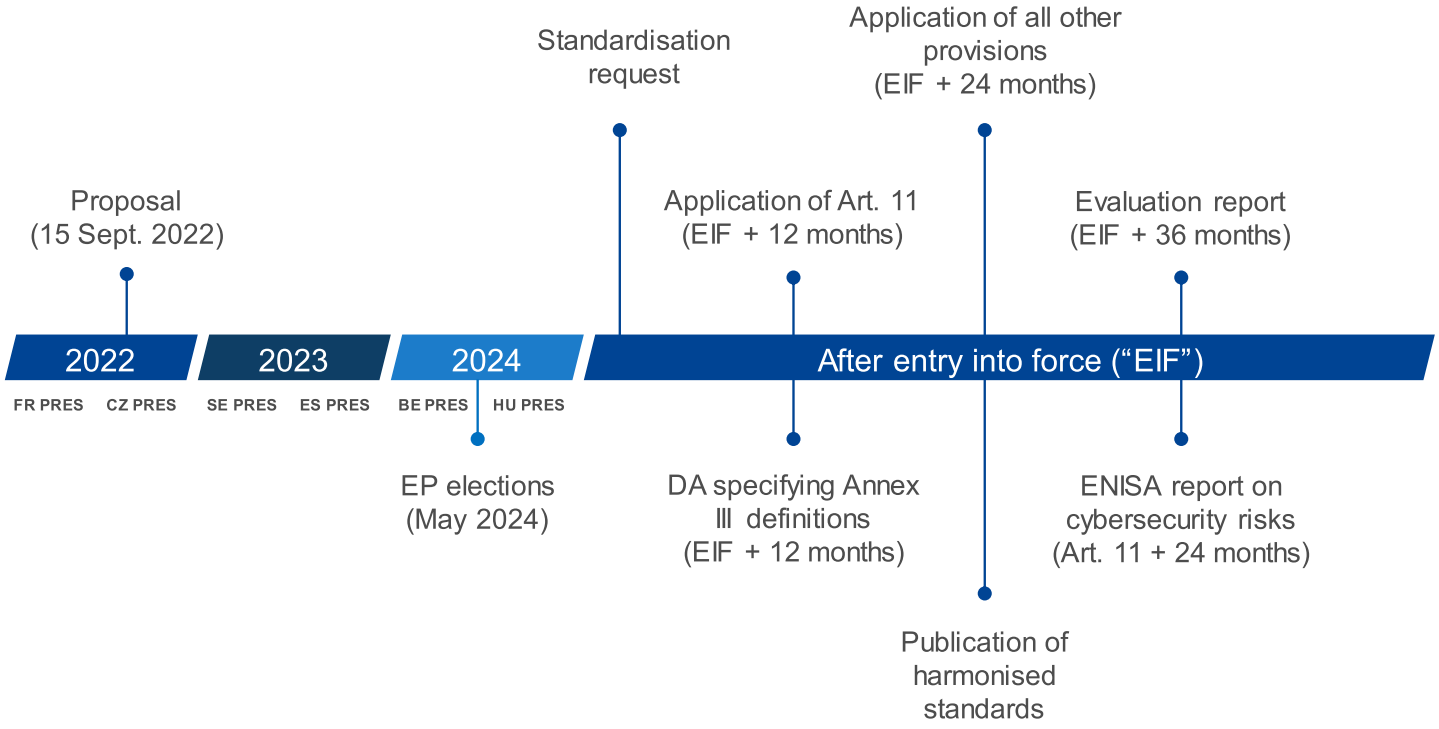
European Commission

Harmonised standards

- Based on **Commission request** according to Regulation (EU) No 1025/2012 + Annual Union Work Programme of Standardisation
- To be developed by **European Standardisation Organisations** (ESOs)
- Steps:
  - ✓ **As of now**, **preparatory work** to start early on in consultation with all relevant stakeholders
  - ✓ EC to adopt standardisation request (comitology procedure) with close consultation of stakeholders and ESOs
  - ✓ 1 months for ESOs to accept (or otherwise) standardisation request
  - ✓ Standardisation work led by ESOs
  - ✓ EC accepts or rejects the harmonised standards

European Commission

Tentative timeline



European Commission

Thank you.