Recent EU cybersecurity legislative initiatives

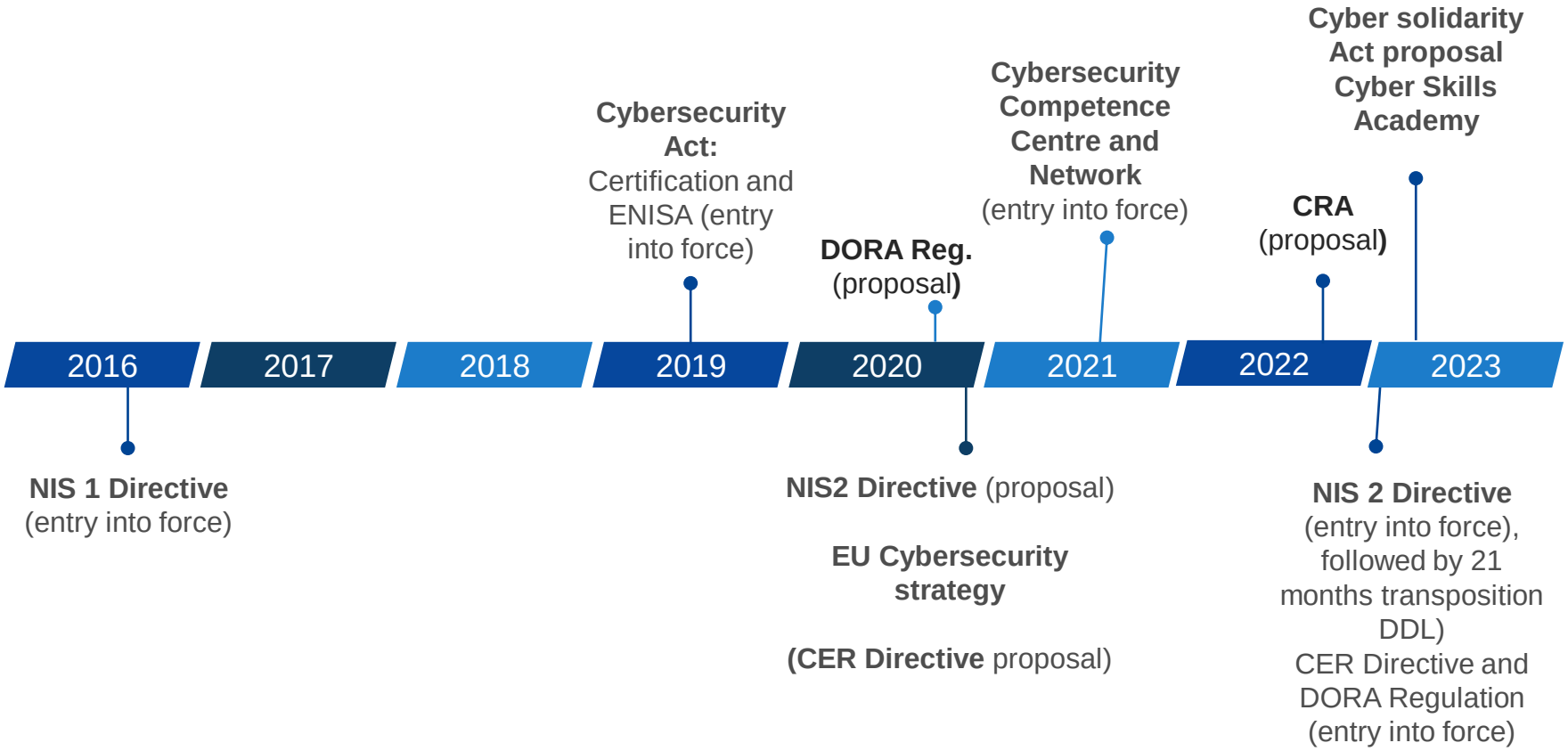
Boryana Hristova-Ilieva, Legal officer
Unit H2 – Cybersecurity and digital privacy policy
DG CONNECT, European Commission

Impact of security incidents - some figures

- 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**.
- **Two thirds** of NIS incidents are the result of a **vulnerability exploitation**. (Other causes are phishing, credential theft etc.)

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

Existing legislative framework



European Commission

Main challenges of NIS 1 Directive

Not all sectors that may be considered critical are in scope

Great inconsistencies and gaps due to the NIS scope being *de facto* defined by MS (case by case OES identification)

Diverging security requirements across MS

Diverging incident notification requirements

Ineffective supervision and limited enforcement

Voluntary and ad-hoc cooperation and info sharing between MS and between operators

Three main pillars of NIS 2 Directive

MEMBER STATE CAPABILITIES

National authorities

National strategies

Coordinated Vulnerability Disclosure (CVD) frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

expanded scope, size threshold

Accountability of top management for non-compliance

Streamlined cybersecurity risk management measures for entities, including **supply chain security**

Streamlined incident reporting requirements

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability database

Peer-reviews

Biennial ENISA cybersecurity report

European Commission

Which sectors are covered by NIS 2?

Annex I	Annex II
Energy (electricity (incl. new categories of operators such as electricity producers, nominated market participants, operators of recharging points), district heating and cooling, oil (incl. central stocktaking entities), gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	RESEARCH **
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, Content Delivery Networks, electronic communications, trust service providers,)	
ICT Service management**	
Public administration entities	
Space	

** additional sectors or sub-sectors agreed by the co-legislators

European Commission

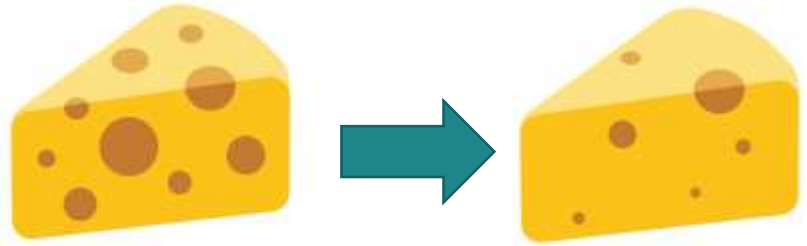
Transposition and implementation of NIS 2

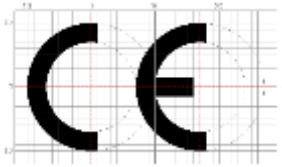
- Transposition by the Member States
- Next steps for the Commission

European Commission

The CRA proposal - main elements

- **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) (product-related, vulnerability handling)
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**





European Commission

CRA 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*

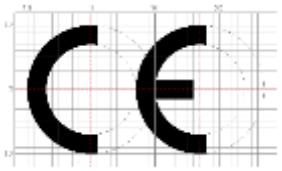
Outright exclusions:

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

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

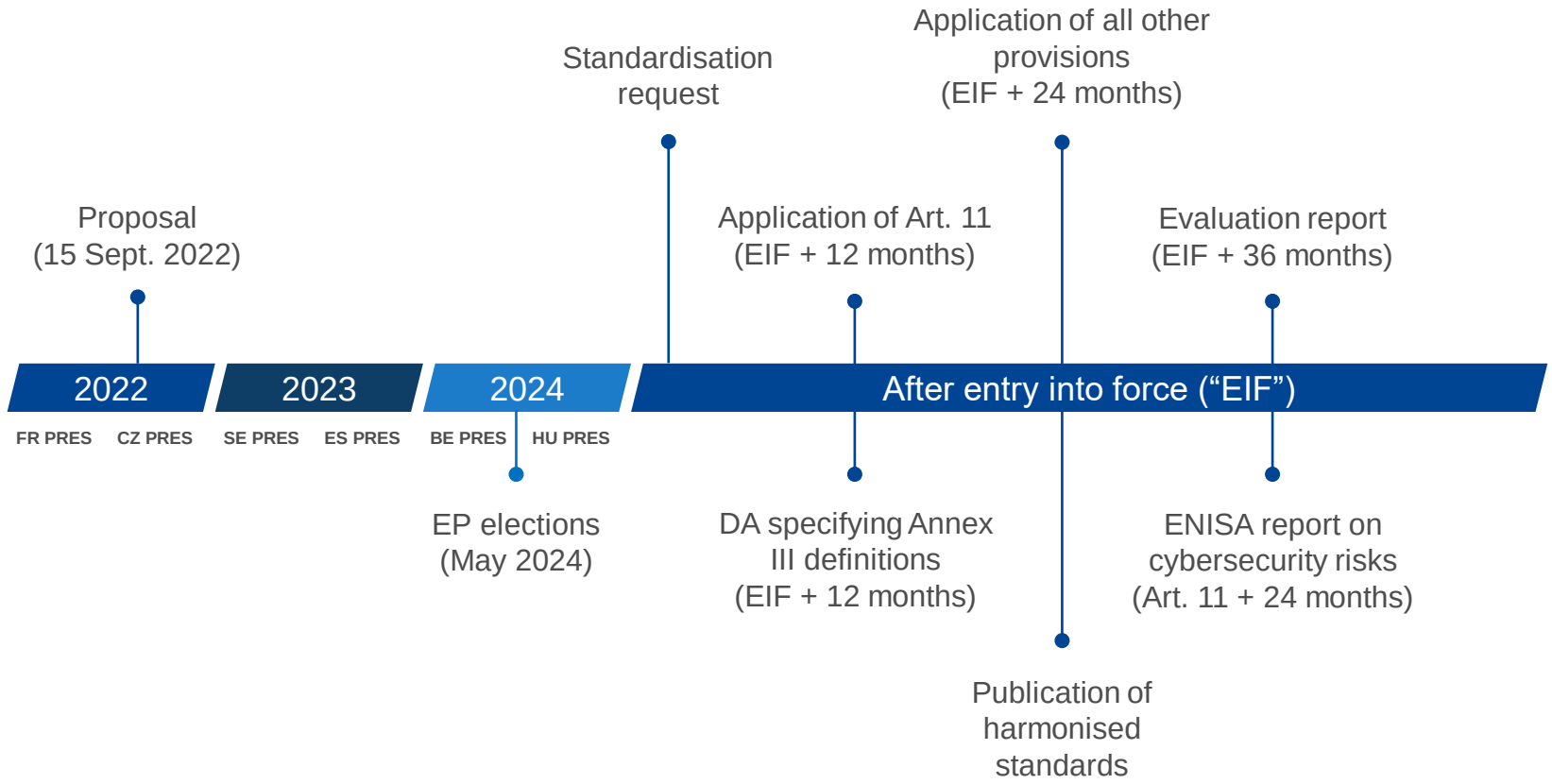
European Commission

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

Tentative timeline



European Commission

Thank you.

European Commission