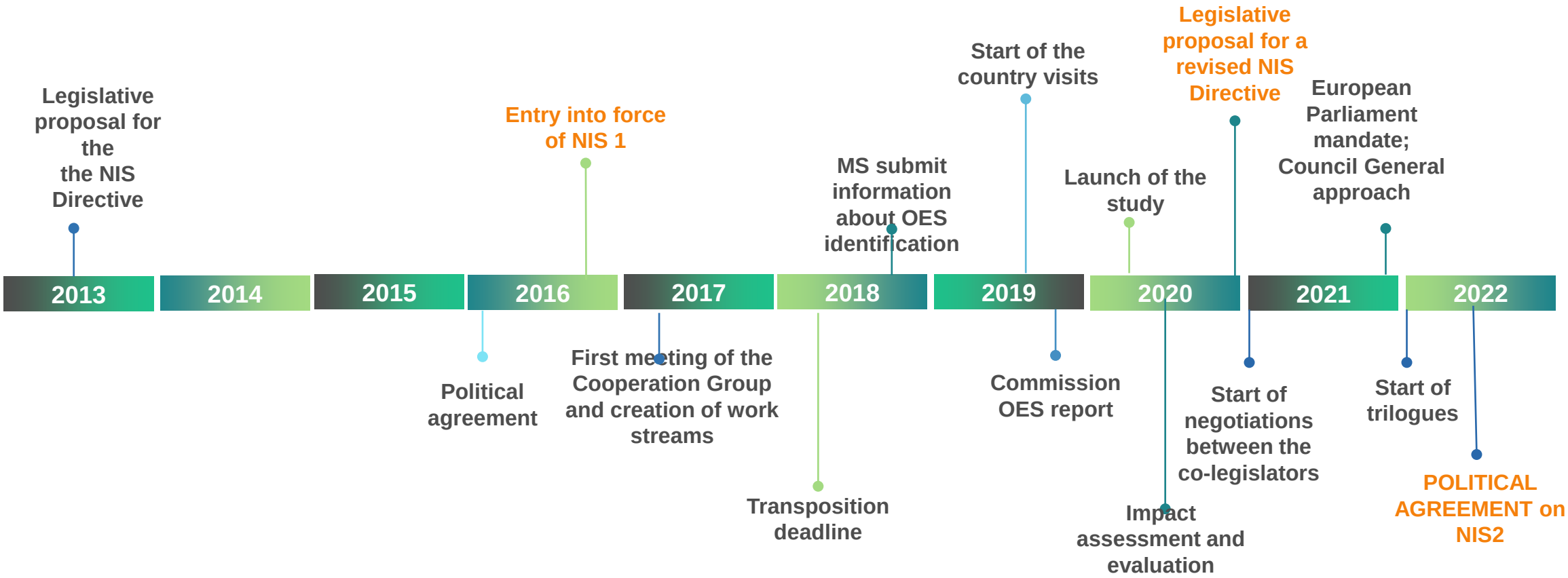
NIS2 & CRA

2nd ENISA maritime cybersecurity conference, Lisbon 14 October 2022

Svetlana Schuster, Head of sector Implementation and Review of NIS Directive, DG CNECT Unit H2

NIS 2 Directive

Timeline of the NIS Directive



European Commission

The NIS 2 vision - main objectives

1

Cover a larger portion of economy and society (**more sectors**)

2

Within sectors: systematically focus on bigger and critical players (**replace current identification process**)

3

Align security requirements (incentivize investments and awareness including by mandating board-level accountability),
expand **supply chain** and supplier relationships risk management

4

Streamline incident reporting obligations

5

Align provisions on national supervision and enforcement

6

More operational cooperation approach including on crisis management

7

Align with proposed
Resilience of Critical Entities Directive

Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES

National authorities

National strategies

CVD frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

Accountability for top management for non-compliance

entities are required to take cybersecurity risk management measures

entities are required to notify significant incidents

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability database

Peer-reviews

Biennial ENISA cybersecurity report

Which sectors are covered?

Annex I	Annex II
Energy (electricity*, district heating, oil (incl. central oil 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

Two regulatory regimes

	Essential entities	Important entities
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities*: ultima ratio* possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the entities are established Exception: telcos - MS where they provide services; Certain digital infrastructures and digital providers – main establishment in the Union.	

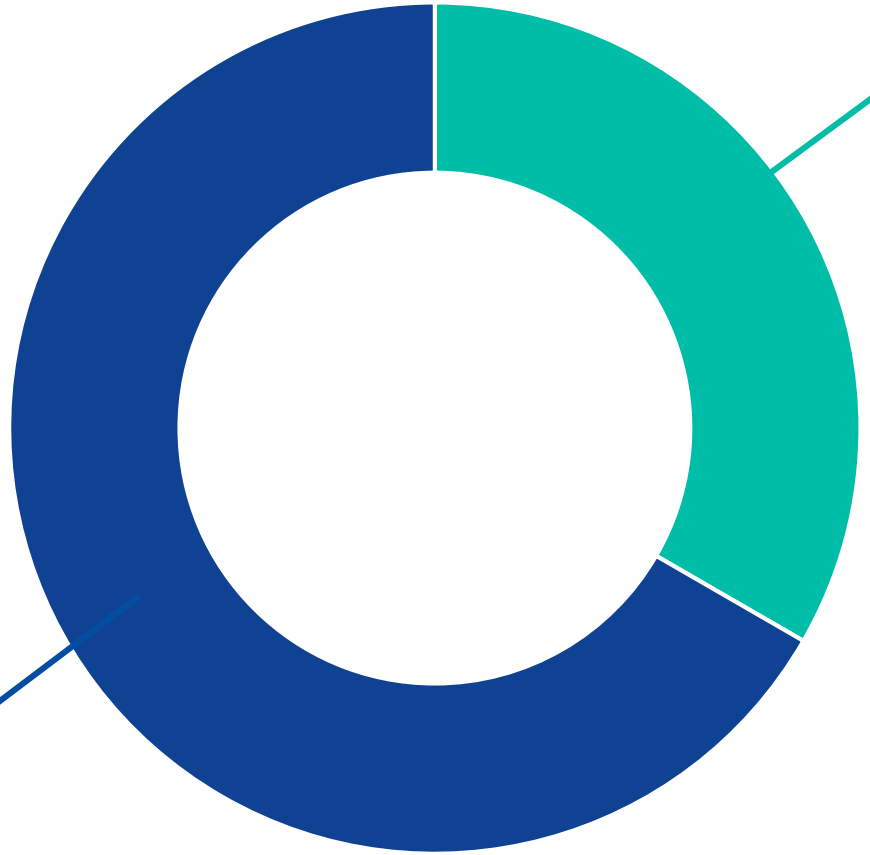
Cyber Resilience Act

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

Role of vulnerabilities in NIS incidents



Other causes
(such as phishing, credential theft etc.)

Two thirds of NIS incidents are the result of a vulnerability exploitation.

Source: ENISA/Gartner (2022)

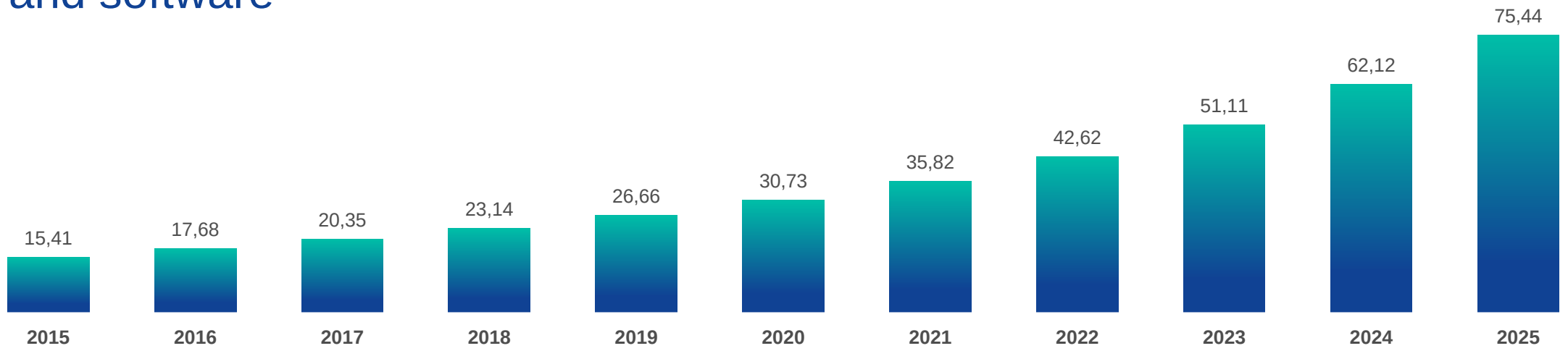
European Commission

Examples of attacks exploiting vulnerabilities

- DDoS (distributed denial of service attacks)
- Ransomware
- Spyware
- Industrial espionage
- Financial theft
- Destructive wipers and malware

Everything is connected

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

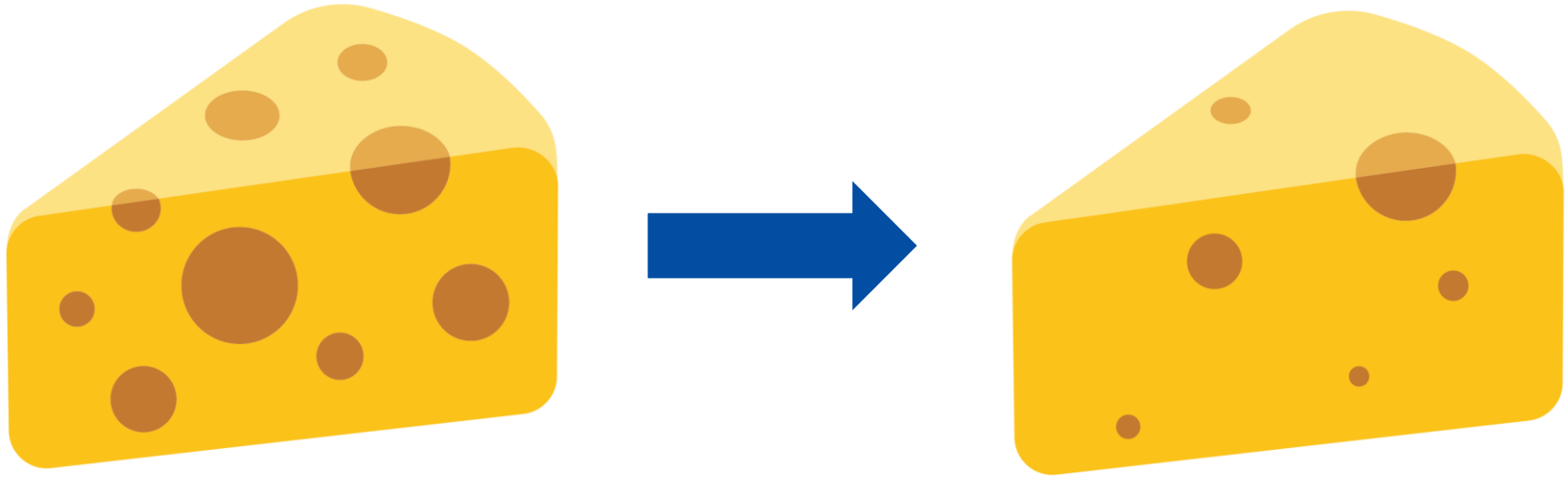


Internet of Things devices worldwide from 2015 to 2025 (in billions)

Source: Forbes/IHS

European Commission

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**

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

Product-related essential requirements

1. Appropriate level of security
2. Products to be delivered without known vulnerability
3. Based on the risk and where applicable:
    - Security **by default**
    - Protection from **unauthorised access**
    - **Confidentiality** and **integrity of data**, commands and programs
    - **Minimisation** of data
    - Availability of **essential functions**
    - Minimise **own negative impact** on other devices
    - Limit **attack surfaces**
    - Reduce **impact of an incident**
    - **Record and monitor** security relevant events
    - Enable adequate **security updates**

Conformity assessment – risk categorisation

- **Default category (90%):** The vast majority of products will be subject to self-assessment (examples: photo editing, word processing, smart speakers, hard drives, games etc.)
- **Critical products (10%):** A small group of critical products listed in the Annex will be subject to *more stringent conformity assessment procedures*, including assessment by an independent third party (examples: firewalls, CPUs, operating systems etc.)
- **Highly critical products:** To future-proof the CRA, the Commission is empowered to adopt secondary legislation requiring *mandatory certification* based on EU cybersecurity certification schemes (Cybersecurity Act) of certain products posing a particularly high risk.

Market surveillance powers and sanctions

- Tools for checks at the disposal of market surveillance authorities (MSAs): documentary checks, requests for information, inspections, laboratory checks etc.
- **When non-compliance found**, MSAs have powers to:

  1) require **manufacturers to bring non-compliance to an end** and eliminate risk;
  2) to **prohibit/restrict the making available** of a product or to order that the product is **withdrawn/recalled**;
  3) impose **penalties** (including fines up to 15 000 000 EUR or up to 2.5 % of worldwide turnover).

- In exceptional circumstances, COM may require ENISA to conduct an evaluation and, based on the results, establish a **corrective or restrictive measure is necessary at Union level** via an Implementing Act (and following MS consultations).

Thank you.