



Cyber Resilience Act

23 November 2022

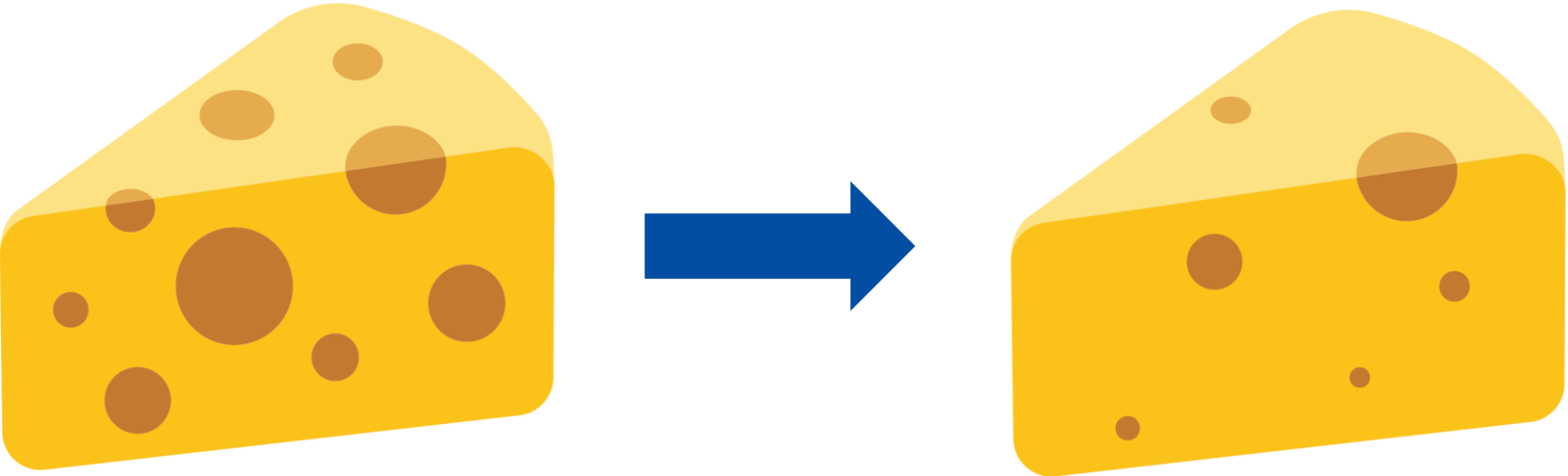
*Maika FOHRENBACH
European Commission, DG CONNECT*

Role of vulnerabilities in NIS incidents



Source: ENISA/Gartner (2022)

CRA in a nutshell



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
- ① 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** – except **remote data processing**

Outright exclusions:

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

Tentative timeline

