NIS 2 – what now?

Lise Fuhr, *Director General*

Norwegian ISOC chapter, 2 March 2023

@ETNOAssociation #ThinkDigital #ETNODigital

ETNO in a nutshell

>70%

Our member's share of the total sector investment; they also employ 525,000 people

30

Countries within the ETNO membership

ETNO has MoUs with international associations (ASIET, US Telecom, ECSO)

10

Working groups & Task Forces chaired by ETNO members and supported by the Office

31

Members

9

Observers

- Influencing policy development processes
- Networking & key contacts
- Sharing best practices
- Events & position papers
- Monitoring & Information

Critical infrastructure put to the test

European leaders blame sabotage as gas pours into Baltic from Nord Stream pipelines

Ursula Von der Leyen warns of 'strongest possible response' to attacks on European energy infrastructure

Russia hacked an American satellite company one hour before the Ukraine invasion

The attack on Viasat showcases cyber's emerging role in modern warfare.

Shetland loses telephone and internet services after subsea cable cut

Police declare major incident as islanders warned it could take days for full services to be restored

etno

The NIS 2 Directive

- Building block of the **EU Cybersecurity Strategy** (December 2020)
- Amends the Directive on security of network and information systems **(NIS)** enacted in 2016, to address its shortcomings.
- Presented along with a new Directive on the resilience of critical entities **(RCE)** that covers ‘offline’ risks, also in telecom networks and services.

Legislative process

Commission proposal
16 Dec. 2020

10 Nov. 2022
European Parliament plenary vote

Council adoption
28 Nov. 2022

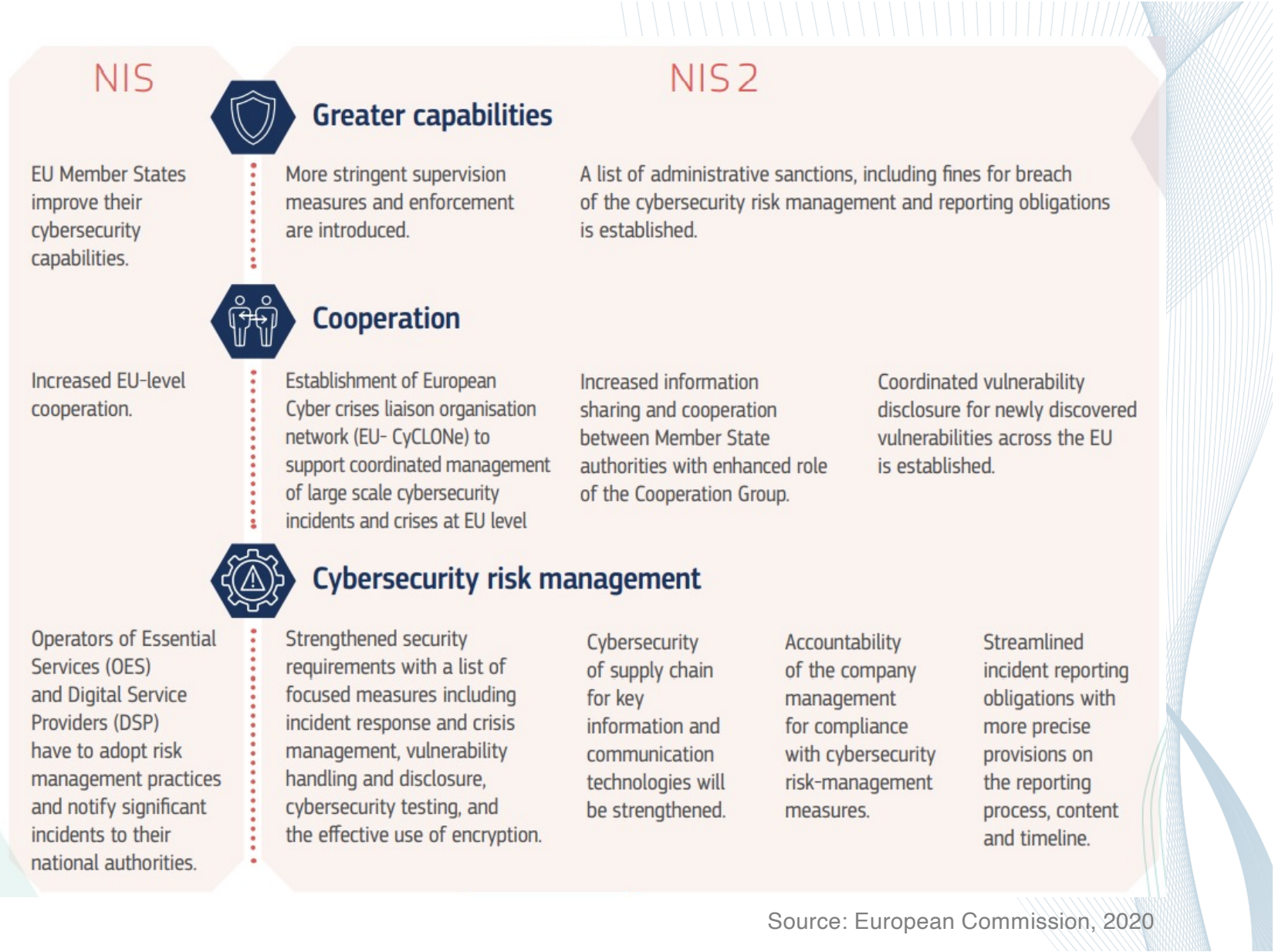
27 Dec. 2022
Publication in the OJ

Entry into force
16 Jan. 2023

What now?

- Member States have to transpose the Directive into national law and directly applicable measures **by 18 October 2024**
- Commission/ENISA **guidelines**
- Commission **delegated and implementing acts**.
- Review of the functioning of the Directive every three years.

NIS2 at a glance



Source: European Commission, 2020

Far-reaching rules

Source: European Commission, 2020

Risk Management measures

- risk analysis and information system security policies;
- incident handling;
- business continuity (e.g., backup and disaster recovery) and crisis management;
- supply chain security including security-related aspects of the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk management measures;
- basic computer hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- human resources security, access control policies and asset management;
- use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate.

Reporting obligations

- Notification of **incident with significant impact** to CSIRT (or CA where relevant) and users if needed.
- Users should be notified of remedies to a **significant cyber threat** that could affect them, and of the threat itself where appropriate.
- Definition of significance of an incident (i.e., severe disruption or financial loss, and considerable material or non-material loss to people and organizations).
- Staged **deadlines** (24h for early warning; 72h for initial notification; 1 month for final report).
- Compulsory feedback by CSIRT/CA.
- CSIRT/CA notification of **cross-border incidents** to other Member States and ENISA, and the public if needed.

Impact on Telecom Operators

- Inclusion of electronic communication providers in scope of horizontal rules and repeal of sectorial security provision.
- Existing national guidelines and legislation for telecom providers should be used for NIS 2 transposition.
- ENISA can develop guidance on security and reporting requirements for telecom providers.

Need for EU-wide guidance and legislation to avoid inconsistency and promote greater harmonisation

Impact on the Internet infrastructure

- Scope includes **top-level-domain (TLD) name servers, public DNS resolvers and authoritative DNS servers**.
- They are under the **jurisdiction** of the Member State where they have their EU establishment (no double sanction for the same infringement).
- The Commission must specify the cybersecurity risk management measures and reporting obligations for DNS providers and TLD registries via **implementing acts** (higher harmonization) by October 2024.
- Foreign players that are not established in the EU but offers services in the Union should designate a **representative**.
- Member States should require that TLD name registries and DNS services collect and maintain accurate and complete domain name registration data in a **dedicated database** and fulfil **legitimate access requests** about specific data within 72 hours. Policies and procedures should be made public.

The crucial role of ICT supply chain

Figure 5: Root cause categories – Telecom security Incidents in 2020

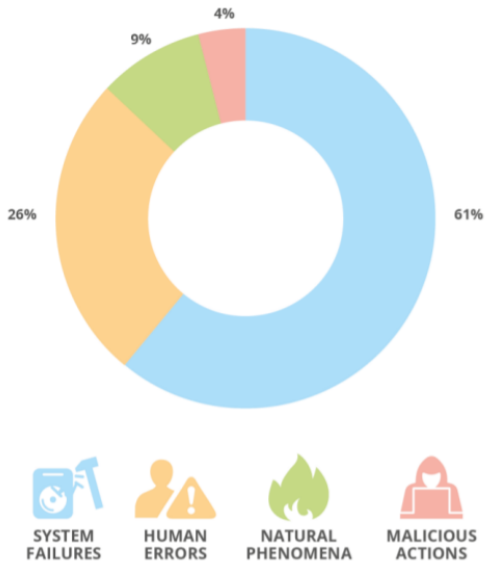


Figure 6: Root cause categories – Telecom security Incidents in 2020

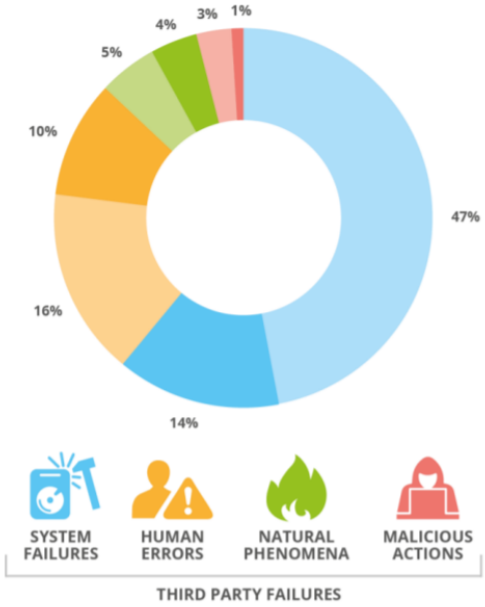
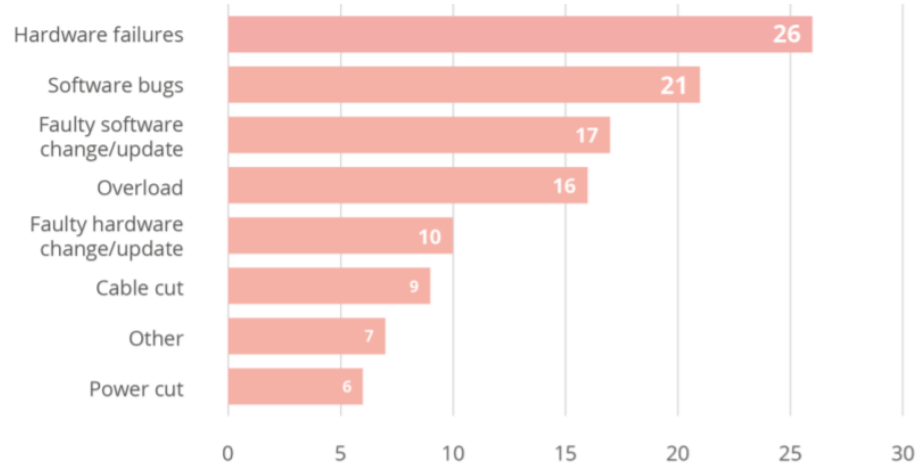


Figure 9: System failures – detailed causes



Source: ENISA Telecom Security Incidents 2020

Greater emphasis on Supply Chain

- **National cybersecurity** strategies including a policy addressing cybersecurity in the ICT supply chain of regulated entities.
- **EU-wide risk assessments of critical supply chains**, to chart the threats of the key ICT services, systems and products used in each sector.
- **Coordinated vulnerability disclosure** improving information sharing between entities and suppliers, and European vulnerability registry managed by ENISA.
- Regulated entities to **assess the quality and cybersecurity practices of their suppliers** during their continued business relationship.
- Possibility to demand that regulated entities use ICT products, services, or processes bearing **EU cybersecurity certification schemes**.
- Inclusion of **Managed service providers (MSP) and Managed Security service providers (MSSP)** in the scope as essential entities.

What next? The Cyber Resilience Act

- Proposal for a **regulation** on horizontal cybersecurity requirements for products with digital elements presented on 15 September.
- **Objective**: increase the cybersecurity of devices with digital elements by establishing common requirements applicable from the design phase throughout the product's entire life cycle.

  - rules for the placing on the market of products with digital elements to ensure cybersecurity;
  - essential requirements for the design, development and production of products with digital elements;
  - essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products during the whole lifecycle;
  - rules on market surveillance and enforcement of the requirements.

- Specific obligations for **critical products**: complementarity with NIS 2.

European Telecommunications
Network Operators' Association

info@etno.eu
Tel: +32 (0)2 219 3242

www.etno.eu