2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION PANEL SERIES

NIS2 AND CRITICAL SECTOR RESILIENCE: WHERE ARE WE - EXPERTS PERSPECTIVES

1. INTRODUCTION

In December 2024, the European Union Agency for Cybersecurity (ENISA) released the 2024 Report on the State of Cybersecurity in the Union, adopted in cooperation with the European Commission and the NIS Cooperation Group, gathering all EU Member States to cooperate on cybersecurity strategic matters. The Report provides an **in-depth analysis of current challenges and opportunities** for strengthening cybersecurity in the European Union. **ENISA is organising a series of policy panels** at key cybersecurity conferences throughout 2025, with the aim to dive deeper into the Report's six key recommendations and foster discussions on the steps required to implement them.

A panel took place on May 7, 2025, at the 4th NISDUC Conference, where experts gathered to exchange insights on enhancing the cybersecurity maturity of sectors covered under the NIS2 Directive.

This paper presents the main discussion points and conclusions from that event.

2. BACKGROUND

In December 2024, ENISA released the 2024 Report on the State of Cybersecurity in the Union. The report offers an in-depth analysis of the current challenges and opportunities for enhancing cybersecurity across the European Union. In addition, ENISA recently published the NIS360 Report, an **assessment focused on sectors covered by the NIS2 Directive**.

2024 State of Cybersecurity Report: Problem Statement

- The NIS1 and NIS2 Directives cover a **wide range of diverse sectors, each with its own criticality, maturity, and specific cybersecurity needs**. All sectors face heterogeneity in terms of entity size and criticality, making it challenging for national authorities to supervise and enforce uniform security requirements.
- The **interconnected digital age** leaves **no sector immune to cyberattacks**. According to the ENISA Threat Landscape report 2024, a significant number of incidents have been observed targeting organizations in **public administration** (19%) and **transport** (11%) sectors. Incidents targeting **digital infrastructure** and **banking** constituted a substantial portion, representing 9% and 8% respectively of total events. A considerable number of events were recorded targeting **civil society**, labelled as 'general public', accounting for 8% of all observed events.
- The **lack of information sharing and collaboration between entities and authorities** also complicates operational cooperation in the event of a crisis.

In response to the identified challenges, the Report includes the following recommendations:

- **Enhance the understanding** of sector-specific characteristics and needs
- **Improve** the level of cybersecurity maturity in **sectors covered by the NIS2 Directive**
- Utilize the **Cybersecurity Emergency Mechanism** (established under the Cyber Solidarity Act) to:
  - Strengthen sectorial preparedness and resilience
  - Focus on sectors identified as weak or sensitive
  - Address risks identified through EU-wide risk assessments

3. THE EXPERT PANEL

Panel Title: NIS2 and Critical Sector Resilience: Where Are We?

Moderator: Paul Timmers, KU Leuven
Panellists:

- Sheila Becker, Institut Luxembourgeois de Régulation
- Karl Dobbelaere, Centre for Cybersecurity Belgium
- Florent Lesueur, Centre Hospitalier du Nord
- Joseph Mager, Nederlandse Spoorwegen
- Jasper Nagtegaal, Rijksinspectie Digitale Infrastructuur

The panel explored key insights from the implementation of the NIS2 Directive and identified opportunities for cross-sector improvement and deeper resilience.

4. KEY INSIGHTS

Disclaimer: The views and opinions expressed by the panellists are those of the individual experts and do not necessarily reflect the official position of ENISA.

Cross-Sector Lessons

- Regardless of the sector, **information sharing** among peers and beyond is crucial.
- The creation of **Information Sharing and Analysis Centers (ISACs)** was highlighted as an effective model.
- **Supply chain visibility** remains a major challenge across sectors.

Knowledge Transfer

- Emphasis was placed on **cross-sector knowledge transfer** to avoid silos and promote shared learning.
- The process of **harmonized identification of essential and important entities** across the EU remains resource-intensive.

Unified Reporting and Spill over Benefits

- Unified reporting improves data quality and fosters **positive spill over effects**—encouraging voluntary adoption of NIS2-aligned practices even by non-obligated entities.
- Some operators fail to report incidents, highlighting the need to foster a reporting mindset and dispel the misconception that reporting leads to penalties or enforcement.

Cultural Shift in Cybersecurity

- A cultural transformation is still needed in many organizations to fully embed cybersecurity as a core element of survival and growth, not just compliance.

Collaboration and Sector-Agnostic Approaches

- The panellists endorsed sector-agnostic collaboration, where companies and authorities across domains work together, e.g. port ecosystems demonstrate effective cross-sector coordination.
- Sharing practices across maturity levels helps **both developing and advanced sectors**.

Sector-Specific Impacts and Risk Assessments

- Impact perception and vulnerabilities vary significantly depending on sector (e.g. water sector vs. digital infrastructure).
- **Entity- or sector-led risk assessments** are essential, as each context requires tailored understanding.

Building on Existing Safety Cultures

- Sectors with established **safety compliance frameworks** (e.g. energy, railways) are well-positioned to integrate cybersecurity into existing practices.
- This integration helps foster cyber awareness and ownership among staff.

National Perspectives:

The **Port of Rotterdam**, functioning as a **unique ecosystem** encompassing multiple sectors, engaged with various **regulatory authorities** to coordinate its approach—**fostering internal coherence**. The **NIS2 Directive** was interpreted through the shared objective of **resilience**. This perspective supports the **holistic configuration of supply chains** within such interconnected ecosystems.

In **Luxembourg**, the **Institut Luxembourgeois de Régulation (ILR)** oversees all sectors **except finance**, ensuring a broad regulatory scope.

The **conference** occurred shortly after a **major electricity outage** affecting **Spain and Portugal**. In response, the panel examined whether **sector-specific cyber emergency management** remains optimal. The consensus pointed toward an **"all-hazard approach"**—an integrated framework that aligns **cybersecurity with broader safety and risk management** practices.

Preparedness was highlighted as a critical component of **crisis management**, with panelists emphasizing the importance of **systematic rehearsals and exercises**. These practices not only expose **vulnerabilities** but also embed **procedural familiarity ("muscle memory")** into

organizational response strategies. **National experiences** were discussed: for instance, the **Netherlands** is planning a **72-hour cross-sector preparedness exercise**.

The conversation also addressed the role of **national audit bodies** in **harmonizing cybersecurity reporting**. **Luxembourg** was cited for its proactive approach in providing **standardized templates** for aligning **security measures** and **maturity assessments** across sectors, along with **self-assessment tools**.

In the **health sector**—where **data flows are predominantly electronic**—returning to **paper-based operations** during a cyber incident poses significant challenges. Therefore, panelists recommended maintaining **printed copies** of **cyber incident response plans**, including **up-to-date contact lists**.

In the **railway sector, interoperability standards** are now being expanded to incorporate **cybersecurity processes and measures based on ENISA's guidance**, demonstrating the sector's alignment with broader **resilience strategies**.

5. CONCLUSIONS

The panel also reflected on the **future beyond the implementation of the NIS2 Directive** and concluded that the **community and sectors could benefit more from shared, bottom-up initiatives** rather than relying solely **top-down legislative approaches**.

In conclusion, **every sector**, even those **not within the scope of the NIS2 Directive**, should **cultivate a strong culture of cybersecurity**.