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

COORDINATING EU CYBERSECURITY SUPPORT FOR NIS2 IMPLEMENTATION - WITHOUT ADDING BUREAUCRACY - 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.

One of these panels took place on October 7, 2025, during the it-sa Expo, where experts exchanged views on how to strengthen the EU's capacity for coherent cybersecurity implementation.

This paper summarizes 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.

The 2024 ENISA State of Cybersecurity Report outlines several challenges currently facing the EU's cybersecurity landscape:

- **expansion in scope** and coverage between the NIS1 and NIS2 Directives significantly **increases the burden on both companies and supervisory authorities**. The policy implementation process remains demanding in terms of time, expertise, and resources.
- the parallel adoption of substantial EU horizontal legislation, such as the Cyber Resilience Act (CRA) or the Cyber Solidarity Act (CSOA), introduces risks of overlap and fragmentation.

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

- **Strengthening the technical and financial support** given to European Union Institution, Bodies and Agencies (EUIBAs) and national competent authorities and to entities falling within the scope of the NIS2 Directive **to ensure a consistent, comprehensive, timely and coherent implementation of the evolving EU cybersecurity policy framework** using already existing structures at EU level such as the NIS Cooperation Group, CSIRTs Network and EU Agencies.

3. THE EXPERT PANEL

Panel Title: Coordinating EU Cybersecurity Support for NIS 2 Implementation - without adding bureaucracy.

Moderator: Christina Rupp, interface
Panellists:

- Hans de Vries, Chief Cybersecurity and Operations Officer, ENISA
- Dr. Judith Nink, Head of Section Cyber Security for Enterprises, BSI
- Jurriën Norder, Head of The Netherlands Cybersecurity Coordination Centre
- Susanne Dehmel, Member of the Executive Board, Bitkom

The discussion centred on three main themes: identifying key challenges and enablers; achieving regulatory coherence and simplification; and leveraging existing EU structures to ensure consistent, efficient implementation.

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.

Challenges and enablers

One of the **pressing issues** identified by the panel was the **uncertainty among companies regarding their obligations under NIS2**. Many organisations, especially those that were not previously categorised as critical infrastructure under NIS1, are still unsure whether they fall within the scope of the new directive. The lack of clarity underscores the **need for detailed, practical guidance from national authorities,** to help companies "catch up" to the expected level of cybersecurity maturity.

From the supervisory side, experts emphasised that **scaling processes and resources is a growing challenge**. As more entities come under the purview of NIS2, national authorities must adapt their supervision models to manage broader oversight efficiently. Instead of one-to-one monitoring, **authorities are increasingly seeking ways to disseminate information and best practices at scale**, ensuring consistency while remaining efficient.

It was argued that **public funding can serve as an important enabler in this process**, but only if it is targeted and tied to measurable outcomes. The discussion highlighted the importance of understanding "**the true price of securing assets**", suggesting that **cybersecurity should be viewed not just as a compliance cost but as an investment with quantifiable value**.

From ENISA's perspective, it was noted that **NIS2 should not be seen as a complete reinvention of the wheel**. The foundation built under **NIS1 provides a valuable starting point, with many of the "most important basics already covered."** However, **scaling capacity to meet the demands of the evolving EU cybersecurity framework remains a challenge** because the Agency itself has not expanded significantly in recent years, even as its mandate and responsibilities have grown.

Regulatory coherence and simplification

A recurring theme throughout the discussion was **the need for coherence across the EU's increasingly complex cybersecurity legal landscape**. Experts underlined that while alignment at the EU level is essential, national authorities must retain responsibility for enforcement. The division of responsibilities should be clear: **the EU should provide overarching frameworks, particularly for incident reporting and notification, while Member States focus on operational oversight and implementation**.

It was also pointed out that **companies operating across multiple Member States often struggle with varying national interpretations of EU rules**. For businesses, consistent implementation is not a matter of legal theory but of practical necessity. Simplifying and aligning reporting obligations across legal acts, such as NIS2[1], DORA[2], CER[3], CRA[4] and GDPR[5] would significantly reduce administrative overhead.

Participants also stressed that **simplification, in their view, does not mean deregulation but smarter regulation**. The growing complexity of EU legislative initiatives may lead to confusion if not properly aligned. On the issue of funding, the Panel called for a debate to find the right balance between resilience and innovation.

All panellists agreed that **excessive layering of rules and sector-specific requirements risks creating confusion and compliance fatigue**. Instead, the **focus should be on interoperability, clarity, and the avoidance of overlapping obligations,** especially in areas such as incident reporting, certification, and supply chain cybersecurity requirements.

[1] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2555.
[2] See https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
[3] See https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[4] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
[5] See https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Leveraging EU Structures for Coordinated Implementation

The discussion also examined how existing EU structures can be used more effectively to support aligned NIS2 implementation. Several speakers called for a **more holistic and agile mandate for ENISA**, allowing it to act **not only as a coordinating and advisory body but also as a forward-looking enabler of cybersecurity strategy and capability development**.

It was further emphasised that while **ENISA plays a key role at the EU level, National Coordination Centres (NCCs) must also operate coherently across Member States**. A model was proposed by one of the experts where "the same line of text" serves as the baseline for NCCs, ensuring consistency in the services and products they offer. However, merging the functions of ENISA, the European Cybersecurity Competence Centre (ECCC), and the NCCs was viewed as counterproductive. Instead, their roles should be clearly defined and complementary.

Panellists also noted that **ENISA could take on a stronger advisory role, particularly in facilitating knowledge exchange and developing best practices for national authorities**. Trust and personal relationships remain essential to effective cooperation across borders.

Finally, **the importance of public–private partnerships (PPPs) in achieving NIS2 objectives** was highlighted. Such partnerships **demonstrate how PPPs can help build trust, share expertise, and accelerate cybersecurity maturity among private actors**. However, greater coordination is needed between national and EU-level initiatives to maximise their impact and avoid duplication of effort.

5. CONCLUSIONS

The panel's discussion converged on several core principles for ensuring that NIS2 implementation strengthens European cybersecurity without adding unnecessary bureaucracy.

- **Coherence must not come at the cost of flexibility** - the EU should make full use of its existing coordination mechanisms, such as the NIS Cooperation Group, the CSIRTs Network, CyCLONE and ENISA's technical expertise to provide guidance and share best practices that promote coherent implementation of NIS2 across Member States. This approach can ensure consistency without creating new regulatory layers.
- **Cooperation and partnership are essential** - public–private partnerships, as well as cooperation between EU and national institutions, are key to sharing expertise and ensuring that both the public and private sectors benefit from the EU's collective cybersecurity resources.
- **Simplification of overlapping frameworks remains a priority** - the interaction between NIS2, GDPR, CER, CRA, the AI Act, and eIDAS2 should be managed to minimise duplication, especially in areas such as incident reporting and compliance monitoring. Streamlined reporting channels and shared databases could significantly ease the administrative burden on companies and authorities alike.
- **Institutional empowerment is crucial** - ENISA and the NCAs need the resources, mandates, and flexibility to fulfil their expanding roles effectively. A stronger, better-connected network of EU cybersecurity institutions can help deliver coherent, high-quality support to Member States and private entities, fostering both resilience and innovation.

The Panel agreed that simplifying regulation is crucial. The goal is not more rules, but better coordination and smarter implementation. The **guiding principle for Europe's cybersecurity framework should be** "**as simple as possible, as strict as necessary**".