enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY
20 years!

2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION

NIS2 ARTICLE 18

1. ENISA shall adopt, in cooperation with the **Commission** and the **Cooperation Group**, a **biennial** report on the state of cybersecurity in the Union and shall submit and present that report to the **European Parliament**. The report shall, inter alia, be made **available in machine-readable data** and include the following:

   a) a Union-level cybersecurity **risk assessment**, taking account of the **cyber threat landscape**;

   b) an assessment of the development **of cybersecurity capabilities in the public and private sectors** across the Union;

   c) an assessment of the general level of **cybersecurity awareness and cyber hygiene** among citizens and entities, including **small and medium-sized enterprises**;

   d) an aggregated assessment of the outcome of the **peer reviews** referred to in Article 19;

   e) an aggregated assessment of the level of **maturity of cybersecurity capabilities and resources across the Union, including those at sector level**, as well as of the extent to which the Member States' **national cybersecurity strategies are aligned**.

2. The report shall include particular **policy recommendations**, with a view to addressing **shortcomings** and increasing the level of cybersecurity across the Union, and a **summary of the findings** for the **particular period** from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

3. ENISA, in cooperation with the **Commission**, the **Cooperation Group** and the **CSIRTs network**, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).

FACTORS CONSIDERED

Indicators of the EUCSI 2024 with the lowest EU average values and/or highest deviation among EU MS

Individual key findings and gaps from other sources, such as the NIS Investments, NIS 360 and NCSS

Main threats to the Union deriving from the Threat Landscape, Risk Assessment and Foresight

Council of the European Union

NIS COOPERATION GROUP

Specific priorities identified by EU MS, as expressed via the Council Conclusions, a survey to the NIS CG and the Meeting of the National Cyber Security Directors in May 2024

REPORT OUTLINE

CYBERSECURITY LANDSCAPE IN THE UNION

Legislative Context

Union-level Risk Assessment

EU Cyberthreat landscape

CYBERSECURITY CAPABILITIES AT THE UNION LEVEL

National Cybersecurity Strategies

Critical Sector Cybersecurity Capabilities

Cybersecurity Awareness and Cyber-hygiene of EU Citizens

INCREASING THE LEVEL OF CYBERSECURITY

Policy Implementation

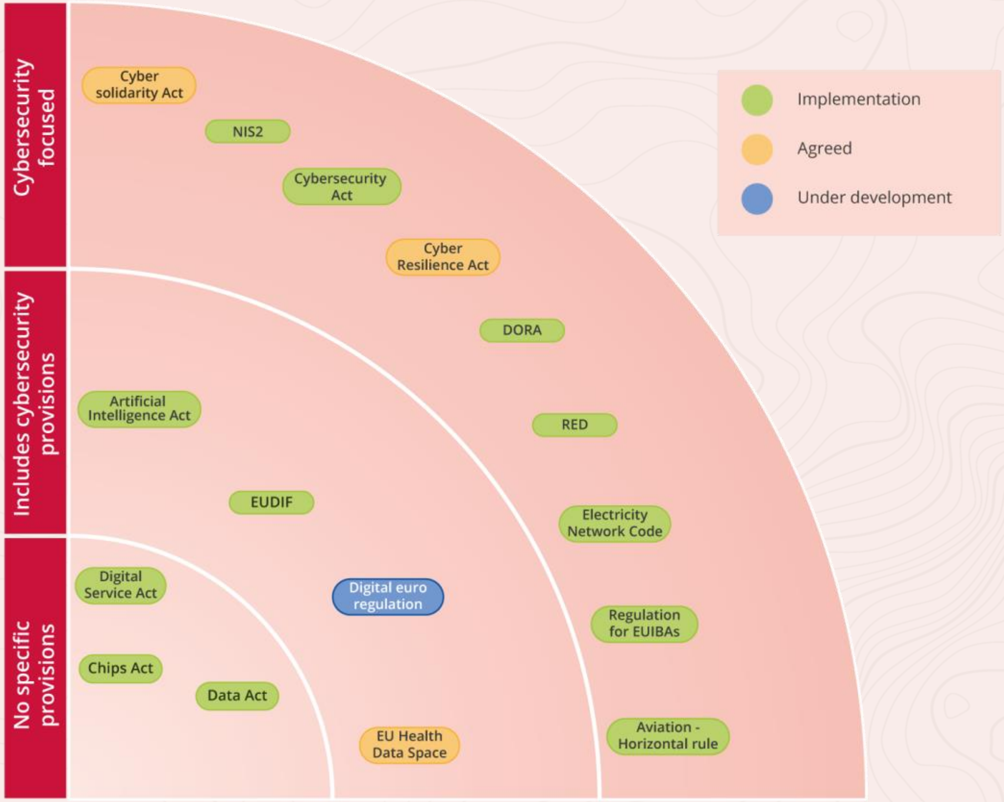
Cyber Crisis Management

Cybersecurity Skills

Supply Chain Security

CYBERSECURITY POLICY LANDSCAPE (in 2024!)

Recent EU policy developments like the *NIS2 Directive, the Cyber Resilience Act (CRA), the Cyber Solidarity Act (CSOA)* have strengthened the EU's cybersecurity framework, setting up structures and processes for advancing EU's cybersecurity posture. At the same time, sectors-specific policies address unique challenges in various critical sectors of our economy and society.



Cybersecurity focused

Includes cybersecurity provisions

No specific provisions

Cyber solidarity Act

NIS2

Cybersecurity Act

Cyber Resilience Act

DORA

RED

Electricity Network Code

Regulation for EUIBAs

Aviation - Horizontal rule

Artificial Intelligence Act

EUDIF

Digital euro regulation

EU Health Data Space

Digital Service Act

Chips Act

Data Act

🟢 Implementation

🟡 Agreed

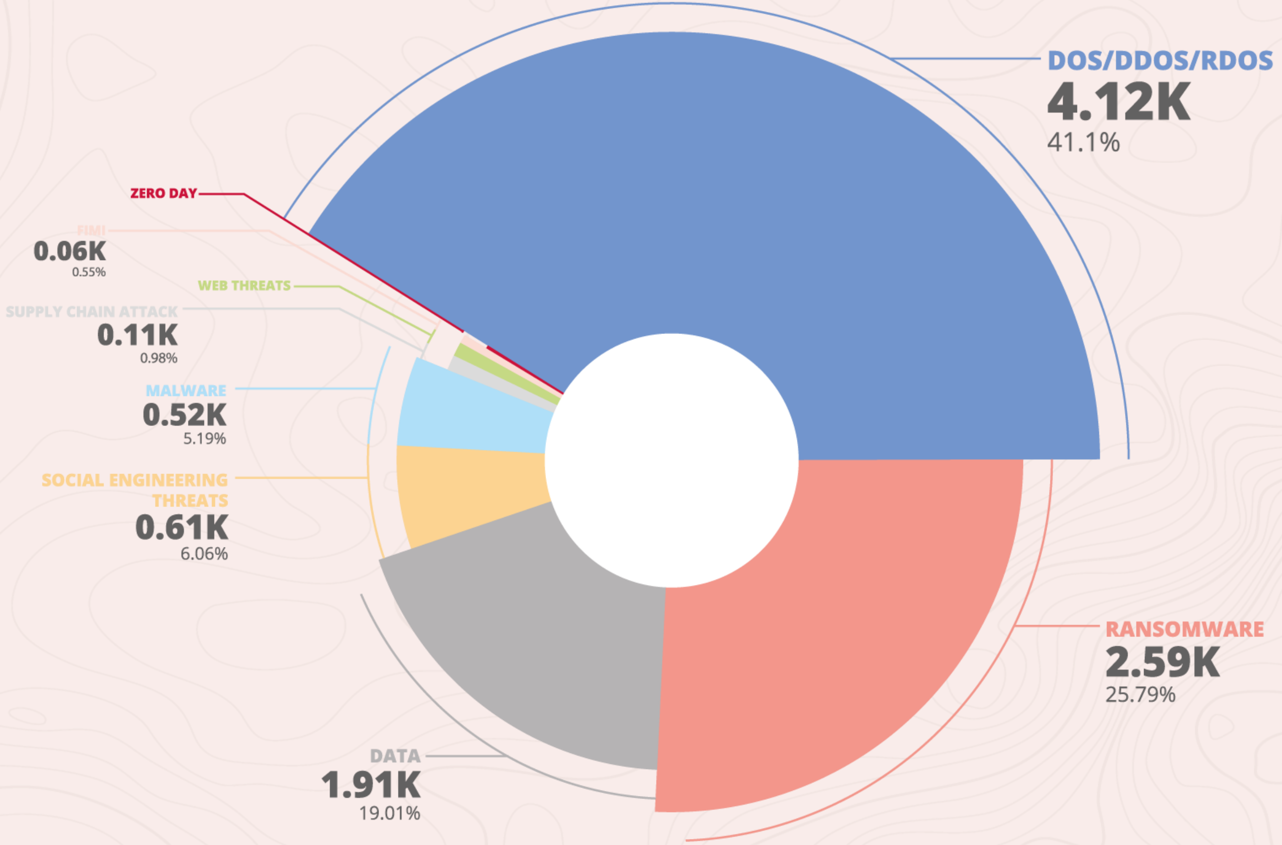
🔵 Under development

EU LEGISLATIVE LANDSCAPE

UNION LEVEL RISK ASSESSMENT

The cyber threat level to the EU during the reporting period was assessed as substantial. Entities are likely being directly targeted by threat actors or exposed to breaches through recently discovered vulnerabilities, making serious disruptions of essential and important entities or EUIBAs a realistic possibility.

INCIDENTS BY THREAT TYPE (July 2023 to June 2024)



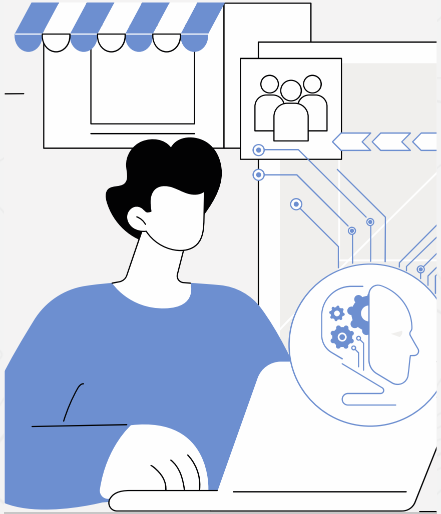
CYBERSECURITY CAPABILITIES AT THE UNION LEVEL

Area	National capabilities: Alignment of national cybersecurity strategies	Private sector capabilities: Capabilities of critical sectors	Societal capabilities: cybersecurity awareness and cyber-hygiene of EU citizens
Findings	Since 2017 all Member States have a national cybersecurity strategy, in some cases also updated in subsequent years. Member States have a different degree of expertise in drafting strategies, ranging from some being at the third (or more) edition of their strategy to some being at their first edition.	All sectors face heterogeneity in terms of entity size and criticality, making it challenging for national authorities to supervise and enforce uniform security requirements. Member States and their national authorities may need to prioritise between the different NIS sectors, deciding which sectors could receive more focus.	People's confidence in their ability to protect themselves from cybercrime decreased, suggesting that cybersecurity awareness has likely increased among EU citizens. Low awareness about cybercrime and relevant reporting mechanisms among EU population. Cybersecurity in higher education: The availability of cybersecurity education programmes varies greatly across EU Member States. Cybersecurity in primary and secondary education: Variations across Member States in term of cybersecurity education maturity.

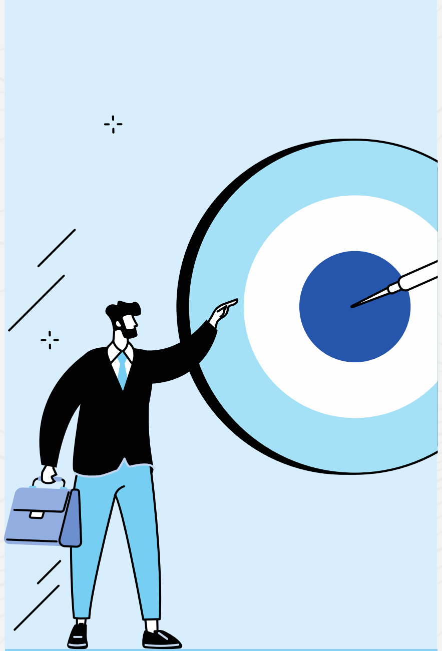
PRIORITY AREAS

Policy implementation including: security measures, incident reporting, vulnerability disclosure

Cyber crisis management including: CSIRTs capabilities, exercises, information sharing



Supply chain



Skills including: education, cyber hygiene

POLICY RECOMMENDATIONS

Strengthening the technical and financial support given to EUIBAs and national competent authorities and to entities falling within the scope of the NIS2 Directive to **ensure a harmonised, 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.

As called upon by the Council, **revising the EU Blueprint for coordinated response to large-scale cyber incidents**, while taking into account all the latest EU cybersecurity policy developments. The revised EU Blueprint should further **promote EU cybersecurity harmonisation and optimisation**, as well as **strengthen both national and EU cybersecurity capabilities** for levelled up cybersecurity resilience at national and European level.

Strengthening the EU cyber workforce by implementing the **Cybersecurity Skills Academy** and in particular by establishing a **common EU approach to cybersecurity training**, identifying **future skills needs,** developing a **coordinated EU approach** to **stakeholders' involvement** to address **the skills gap and** setting up a **European attestation scheme for cybersecurity skills.**

Addressing supply chain security in the EU **by stepping up EU wide coordinated risk assessments** and the **development of an EU horizontal policy framework for supply chain security** aimed at addressing the cybersecurity challenges faced both by the public and the private sectors.

Enhancing the understanding of sectorial specificities and needs, improving the level of cybersecurity maturity of sectors covered by the NIS2 Directive and **using the future Cybersecurity Emergency Mechanism to be established under the CSOA** for sectorial preparedness and resilience with a focus on weak or sensitive sectors and risks identified through EU-wide risk assessments.

Promoting a **unified EU approach**, by building on existing policy initiatives and strategies and by harmonising national efforts to achieve a **common high level of cybersecurity awareness and cyber hygiene among professionals and citizens** irrespective of demographic characteristics.

EU CYBERSECURITY INDEX 2024

The EU average is

62.65

out of 100

Deviation from the EU average

Average

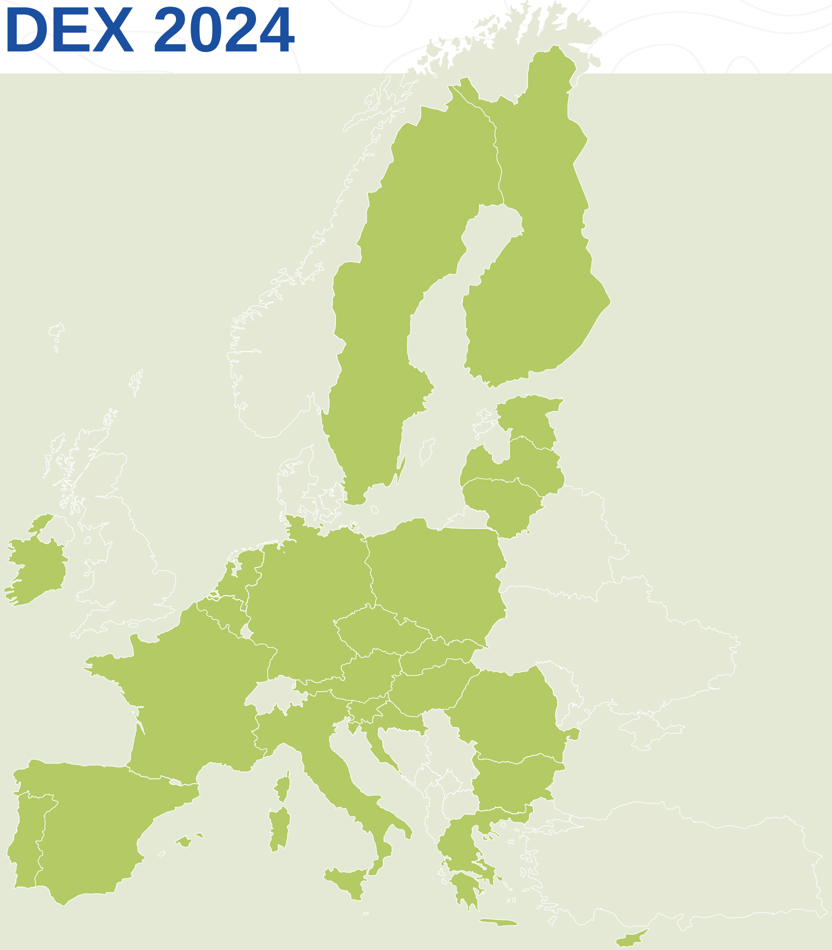
3.76

Maximun

7.45

Minumun

-13.18



LOOKING AHEAD

- Recent significant improvements in the overarching policy framework and established structures for cybersecurity across the EU can provide the **basis for further development of cybersecurity capabilities and enhance cyber resilience and effective cooperation among EU MSs**. In this context the EU and its Member States should maximise the use of these existing structures to tackle any cybersecurity fragmentation and shield the EU against threats.

- National competent authorities and EUIBAs alike are faced with similar challenges when it comes not only to implementing their **new roles but also dealing with the ever-evolving cyber threat landscape**.

- In terms of emerging technologies, two topics have gained traction over the past year, namely AI and Post-Quantum Cryptography (PQC).

- It is critical to **ensure that R&D&I funding is available for critical technologies and applications to support global competitiveness in cybersecurity and to reinforce the EU's cybersecurity capabilities**.

- The de facto cross-border nature of cybersecurity incidents and the risks that come with it could be re-assessed in light of the new technological trends and the geopolitical context affecting the EU. **The national authorities of MSs and EUIBAs need to be prepared to answer tomorrow's challenges in the area of cybersecurity**.

- Particular emphasis could be placed on developing **common situational awareness and operational cooperation**. While the framework already exists, it needs to be tested to identify any potential shortcomings if and when the need for its full deployment arrives.