enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY 20 years!

2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION

CONDENSED VERSION

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION

In cooperation with the NIS Cooperation Group and the European Commission, in accordance with Article 18 of the Directive (EU) 2022/2555 (NIS2).

DECEMBER 2024

AT A GLANCE

The first **report on the state of cybersecurity in the Union** provides EU policy makers with an evidence-based overview of the state of play of the cybersecurity landscape and capabilities in the EU. The report also provides policy recommendations to address identified shortcomings and increase the level of cybersecurity across the European Union. The full report is available on the ENISA website.

DISCLAIMER

The drafting of this report took place in a special period as the collected data refer to a period when the NIS2 transposition was still ongoing, whereas the publication date followed the NIS2 transposition deadline. We acknowledge that this discrepancy is likely to lead to observations and results concerning the NIS2 transposition status and the development of capabilities that may not reflect the respective status as of October 17th and thereafter. Still, it is important to capture a snapshot of the state of cybersecurity in the Union as this transposition process is still ongoing, in order to support the assessment of the impact of NIS2 in subsequent reports.

RECOMMENDATIONS

Strengthening the technical and financial support given to EU institutions, bodies and agencies (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.

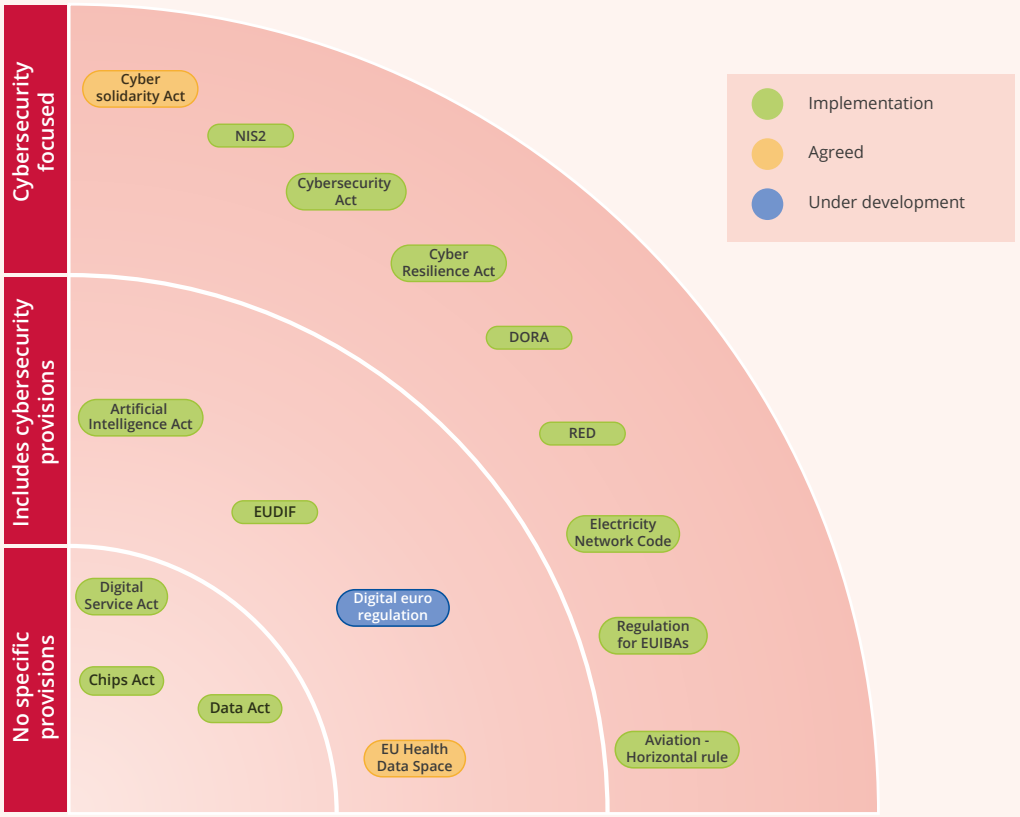
Enhancing the understanding of sectorial specificities and needs, improving the level of cybersecurity maturity of sectors covered by the NIS2 Directive and **using the future Cybersecurity Emergency Mechanism to be established under the CSOA** for sectorial preparedness and resilience with a focus on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

Promote a **unified approach** by building on existing policy initiatives 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.

LEGISLATIVE CONTEXT

Recent EU policy developments like the *NIS2 Directive, the Cyber Resilience Act (CRA), the Cyber Solidarity Act (CSOA) and the Cyber Resilience Act (CRA)*, 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.

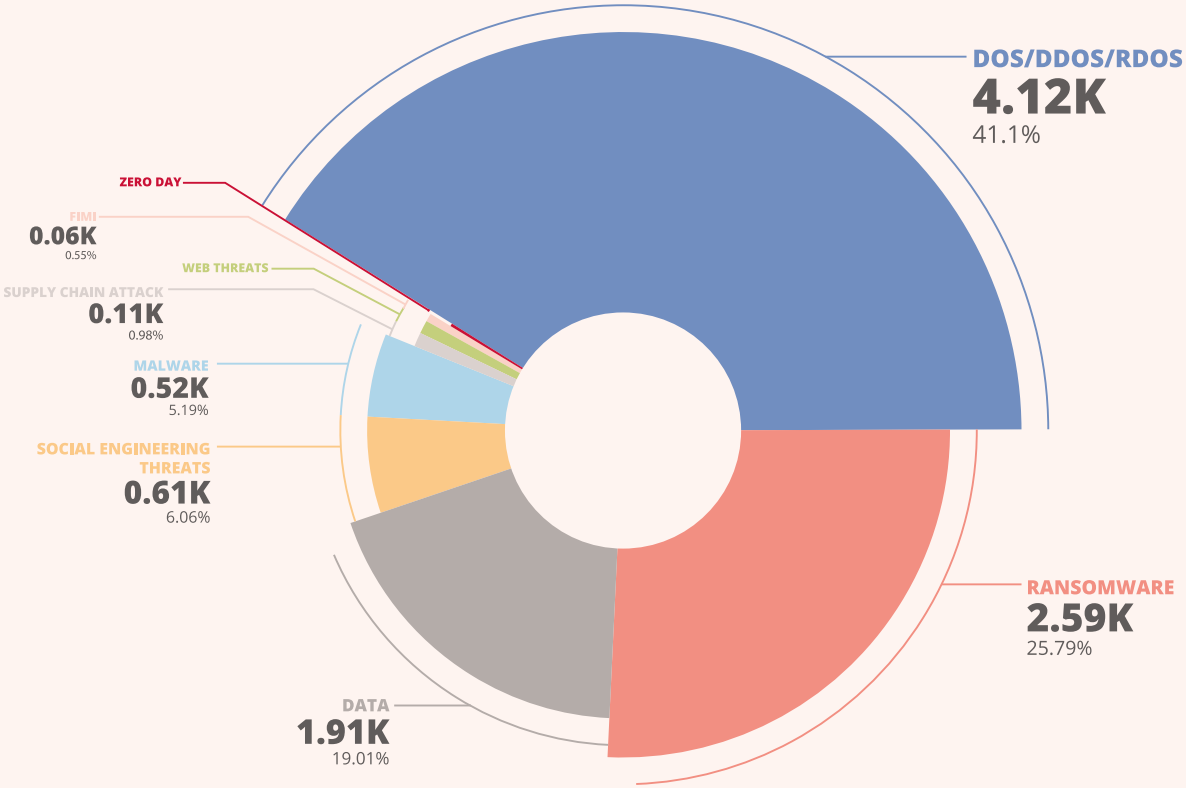
EU LEGISLATIVE LANDSCAPE



UNION LEVEL RISK ASSESSMENT

The cybersecurity threat level in 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

Assessing capabilities in the society, the public and private sectors

Overall, Member States show convergence in their cybersecurity posture, with some countries lagging slightly behind.

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.** **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.

Policy Recommendation:

Promote a unified approach by building on existing policy initiatives 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.

Policy Recommendation:

Enhance the understanding of sectorial specificities and needs, improve the level of cybersecurity maturity of sectors covered by the NIS2 Directive, and use the future Cybersecurity Emergency Mechanism established under the CSOA for sectorial preparedness and resilience focusing on sectors found to be weak or sensitive and risks identified through EU-wide risk assessments.

POLICY IMPLEMENTATION

Enhancing technical and financial support for harmonised implementation

As the EU cybersecurity policy framework has evolved, implementation at a national level becomes a priority and national competent authorities are in the process of working towards this goal. However, the policy implementation process is demanding both in terms of time and resources.

Area	Complementary and coherent policy implementation	Identification and supervision	Cybersecurity risk management measures	Information sharing and reporting obligations
Findings	To prevent fragmentation and overlap in cybersecurity regulations, the Council urges the Commission to map out key EU legislation, including NIS2 and sector-specific acts, and leverage synergies for cohesive implementation across the EU.	The process to establish a list of essential and important entities by the MSs is assessed at 62% with 22 MSs close or above this average. The implementation of supervisory measures varies among MSs and improvements are expected as national transposition efforts progress.	Two-thirds of the MSs have defined cybersecurity baselines for essential and important entities, while the rest are in the process of identifying and documenting them. When it comes to implementation of cybersecurity risk management measures, we observe significant deviations among entities, which are dependent to the size of the company and the maturity of the sector. Top management involvement **in cybersecurity affects significantly whether security measures are implemented. It influences** risk management, incident response, and third-party risk management.	National cooperation is generally strong, with improved collaboration among NIS2 entities. However, cooperation between NIS2 authorities and those under other EU legislation is lagging behind in some areas. Notification obligations and contextual measures are progressing, but some Member States lack reporting tools. Coherent implementation across EU legislation and Member States is essential for effectiveness. Reported incidents have remained steady (EECC) or increased (NIS1, eIDAS), indicating both a growing threat landscape and improved reporting. However, the low numbers suggest under-reporting persists.

Policy Recommendation:

Strengthen the technical and financial support to EUIBAs and 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.

CYBER CRISIS MANAGEMENT

Enhancing harmonised cybersecurity resilience

At the time of the adoption of NIS1, in 2016, EU-level cooperation on crisis management was still a relatively new area. Since then, significant changes have happened, such as the establishment of the EU-CyCLONe network of national cyber crisis management authorities and new provisions in NIS2.

Area	Situational awareness	CSIRTs	Cybersecurity Exercises
Findings	**A common, real-time picture** for all Member States and covering all aspects of situational awareness is missing. **All countries monitor cybersecurity threats, but monitoring frequency and alerting methods vary**. While different alerting modes aren't a major issue, inconsistent monitoring frequency highlights capability gaps in some Member States. **OESs/DSPs' capabilities for information collection and exchange are not yet mature**. Many, especially SMEs, do not have Security Operation Centers (SOCs) and invest little in CTI. However, Information Sharing and Analysis Centers (ISACs) are proving successful for information sharing at the EU level. **Reported cybersecurity incidents likely represent only a fraction of actual incidents**. SMEs, in particular, may underreport due to reputational concerns, lack of awareness. Notably, a strikingly high number of SMEs claim to have experienced no incidents, compared to large enterprises.	CSIRTs Network members are **well-connected internationally** but **could improve in aligning with recognised practices**. This need is even greater for CSIRTs outside the Network. Enhancing the scalability of CSIRTs' tools, especially for process automation, could help harmonize maturity and capabilities across the EU.	While EU-level exercise participation is high, the **lack of structured national exercises may weaken overall EU cybersecurity crisis response**. Exercises are organized under various frameworks, making it crucial to avoid "exercise fatigue" to maintain the effectiveness of this high level of participation.

Policy Recommendation:

As called upon by the Council, the European Commission, when proposing a revision of the EU Blueprint for coordinated responses to large-scale cyber incidents, takes 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 the national and European levels.

CYBERSECURITY SKILLS

Strengthening a common EU approach to cybersecurity skills and trainings

In a fast evolving and geopolitical cybersecurity landscape, promoting a dynamic cybersecurity culture through awareness and improving relevant skills along with adopting initiatives aiming to cultivate and retain cybersecurity talent are crucial aspects for addressing current and upcoming threat challenges.

Area	Cybersecurity skills	Diversity and Inclusion	Cybersecurity training and awareness in Enterprises	Enterprises' Cyber hygiene
Findings	 While the demand for people with ICT and cybersecurity **skills is rapidly increasing**, the cybersecurity skills and talent shortage is growing too.	 **Gender imbalance in cybersecurity roles** in the EU.	 **Enterprises in Europe understand the importance of cybersecurity**, but taking relevant action remains a challenge. SMEs lag in cybersecurity awareness compared to large enterprises.	 The state of cyber hygiene in the EU reveals a concerning **gap between SMEs and large enterprises**.

Policy Recommendation:

Strengthen 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.

SUPPLY CHAIN SECURITY

Stepping up coordination on supply chain security

Threat groups demonstrate a continuous interest and increased capability in supply chain attacks. Strong cybersecurity protection is no longer enough for organisations when attackers have shifted their attention to suppliers.

Area	Vulnerability handling and disclosure	Supply chain security
Findings	Member States are progressing in the definition and implementation of national coordinated vulnerability disclosure (CVD) policies. **37% of MSs have defined a national CVD policy. 55% of MSs are currently in the process of defining CVD policies.** **Operators of Essential Services (OESs) and Digital Service Providers (DSPs) face challenges in handling vulnerabilities for the entirety of their assets or patching in a timely manner.** We expect this gap to grow with the addition of new sectors and entities under NIS2. Such challenges also depend on sectorial characteristics.	**Supply Chain Compromise of Software Dependencies is considered the top emerging threat among the Cybersecurity threats for 2030**. in 2023, there was continuous activity by threat actors using software updates to deliver malware to victims. Currently, **74% of Member States have defined supply chain security measures** in their national legislation. This number is expected to increase further due to the national transposition of NIS2 and **the requirements of the DORA regulation for the finance sector**. In 2023, **77% of OESs and DSPs had a policy manage risks from third-parties**. Large enterprises are more likely to have a policy (85%) compared to SMEs (53%). Even fewer entities have dedicated resources for supply chain cybersecurity. Internationally **the number of cybersecurity certification scheme and assessment methodologies is growing** over the years. **The CRA introduces requirements for products and obligations for manufacturers** that will ultimately result in more secure products to be placed on the EU market.

Policy Recommendation:

Supply chain security should be further addressed by stepping up EU wide coordinated risk assessment and the development of an advanced EU horizontal policy framework for supply chain security, aimed at addressing the cybersecurity challenges faced both by the public and the private sectors.

LOOKING AHEAD

Recent improvements in the EU's cybersecurity policy framework provide a solid foundation for strengthening cybersecurity capabilities, boosting resilience, and improving strategic cooperation among EU Member States.

National competent authorities and European Union Institutions, Bodies, and Agencies (EUIBAs) face similar challenges not only in taking on their new roles but also in managing the constantly changing cyber threat landscape.

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

It is critical to ensure that research, development and innovation funding is available for critical technologies and applications to boost global competitiveness in cybersecurity and to strengthen the EU's cybersecurity capabilities.

The cross-border nature of cybersecurity incidents could be re-assessed in light of the new technological trends and the geopolitical context affecting the EU.

The national authorities of EU Member States and EUIBAs need to be prepared to answer tomorrow's challenges in the area of cybersecurity. Emphasis could be placed on building common situational awareness and seamless operational cooperation. While a policy and legal framework is in place, it should be tested to uncover any potential gaps.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union