enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

20 years!

2024 REPORT

# ON THE STATE OF CYBERSECURITY IN THE UNION

## CONTACT

For contacting the authors please use security-index@enisa.europa.eu For media enquiries about this paper, please use press@enisa.europa.eu.

## AUTHORS

ENISA

## ACKNOWLEDGEMENTS

We would like to thank the NIS Cooperation Group and the European Commission for their invaluable feed-back, review and engaged cooperation.

## LEGAL NOTICE



## COPYRIGHT NOTICE



Catalogue number: TP-01-24-005-EN-N

ISBN: 978-92-9204-681-1

DOI: 10.2824/0401593

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION

DECEMBER 2024

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

This document marks the **first report on the state of cybersecurity in the Union**, adopted by ENISA in cooperation with the NIS Cooperation Group and the European Commission, in accordance with Article 18 of the Directive (EU) 2022/2555 (hereinafter NIS2). The report aims at providing policy makers at EU level with an evidence-based overview of the state of play of the cybersecurity landscape and capabilities at the EU, national and societal levels, as well as with policy recommendations to address identified shortcomings and increase the level of cybersecurity across the Union.

The drafting of this report precedes the transposition date of NIS2. As a result, some of the data presented here may not fully reflect cybersecurity capabilities following the transposition deadline of 17 October 2024. Still, this report includes several data points unlikely to change in the short- and mid-term and serves as a **snapshot of the state of cybersecurity in the Union just before NIS2 is fully implemented** by EU Member States (MSs).

The recent past has been characterised by **horizontal policy initiatives including but not limited to NIS2, CRA, CSOA and EUDIF** that improve the EU cybersecurity policy framework and establish all necessary structures and processes to allow for targeted improvements at the Union level of cybersecurity moving forward. Sectorial policy initiatives (e.g. DORA, NCCS, Aviation) were adopted in parallel to address specific sectorial challenges. At the same time the **volatile geopolitical landscape** has influenced the goals and tactics employed by state and non-state threat actors, while an assessment of the threat landscape reveals an **increase in cybersecurity incidents in the EU** with ransomware and DDoS attacks getting the lion's share among the various types of attack observed.

This report concludes that the maturity of the EU cybersecurity policy framework has reached a considerable level and that **the following period could place emphasis on supporting private and public sector entities with the implementation of the legislation by EU MSs, with the support of the European Commission and ENISA.** The plethora of mechanisms, processes and platforms for collaboration established within this framework, such as the NIS Cooperation Group, EU-CyCLONe and the CSIRTs Network to name but a few, provide a solid basis and a comprehensive toolbox to address the shortcomings identified in key policy areas, namely **Policy Implementation, Cyber Crisis Management Skills** and **Supply Chains**.

## 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 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.

The data contained in this report generally refers to the current legal framework (e.g. NIS2 and the European Digital Identity Framework) unless otherwise specified; for example, use of the terms Operators of Essential Services (OESs) and Digital Service Providers (DSPs) and related data concern NIS1.

## Specifically, this report recommends:

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.

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.

# INTRODUCTION

# INTRODUCTION

Article 18 of the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)[1] foresees that ***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***. This document represents the **first ever** version of this report on the **state of cybersecurity in the Union** to be presented to the stated target audience, the European Parliament.

The data used to assess the state of cybersecurity in the Union and to conduct the analysis in order to identify shortcomings and propose measures to increase the overall level of cybersecurity in the Union comes from several sources, including, though not limited to, the EU Cybersecurity Index, the ENISA Threat Landscapes, the NIS Investments report, the EU Cybersecurity Technical Situation Report on incidents and threats (Cybersecurity Act Article 7 (6) report), the Foresight Cybersecurity Threats for 2030, incidents reported in the context of existing cybersecurity legislation, the evolving EU policy landscape and more[2].

The methodology, including the relevant variables, such as quantitative and qualitative indicators from all data sources considered, has been developed by ENISA in cooperation with the Commission, the Cooperation Group and the CSIRTs network, ENISA's Management Board and ENISA's NLO network.

These sources provide insights into different aspects of cybersecurity in the Union and the observations and findings presented in this report are based on individual data points of interest or a correlated analysis of multiple data points from the aforementioned data sets. The observations and findings have also been validated through a series of consultations with the NIS Cooperation Group and the European Commission.

The report is intended to take stock of the state of cybersecurity in the EU from the entry into force of the NIS2 Directive on 16 January 2023 until July 2024. In exceptional cases, where recent data were not available, older data sources were used.

Articles 18.1 and 18.2 of NIS2 outline specific elements that shall be included in the report. These are mapped to the report structure as follows.

| ARTICLE 18 REQUIREMENTS | MAPPING TO REPORT STRUCTURE |
|---|---|
| **Art 18.1(a):** *a Union-level **cybersecurity risk assessment**, taking account of the **cyber threat landscape*** | Cybersecurity risk assessment in **section 1.2**<br>Cyber threat landscape in **section 1.3** |
| **Art 18.1(b):** *an assessment of the development of **cybersecurity capabilities in the public and private sectors** across the Union* | Union level based on Index findings in **section 2.1**<br>National level capabilities in **section 2.2**<br>Private sector capabilities in **section 2.3** |
| **Art 18.1(c):** *an assessment of the general level of **cybersecurity awareness and cyber hygiene** among citizens and entities, including small and medium-sized enterprises* | In **section 2.4** |
| **Art 18.1(d):** *an aggregated assessment of the outcome of the **peer reviews** referred to in Article 19* | Not covered as the peer review mechanism had not been implemented as of the drafting of the report but will be included in future versions of the report. |
| **Art 18.1(e):** *an aggregated assessment of the level of **maturity of cybersecurity capabilities and resources across the Union, including those at sector level** and the extent to which the Member States' **national cybersecurity strategies are aligned*** | Union level based on Index findings in **section 2.1**<br>Maturity of national level capabilities in **section 2.2**<br>Maturity of private sector capabilities in **section 2.3**<br>Societal cybersecurity awareness and cyber hygiene in **section 2.4**<br>Alignment with NCSS in **section 2.2** |
| **Art 18.2:** ***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* | Policy recommendations in **chapters 2 and 3** where relevant<br>Summary of the EU Cybersecurity Technical Situation Reports in **section 1.2** |

Specifically for the development of policy recommendations, the report presents an in-depth analysis of data points across several selected policy areas. The identification of these areas was based on the main shortcomings observed from the available data, as well as being based on the opinions expressed by EU MSs.

Chapter I

# CYBERSECURITY LANDSCAPE IN THE UNION

## 1.1 LEGISLATIVE CONTEXT

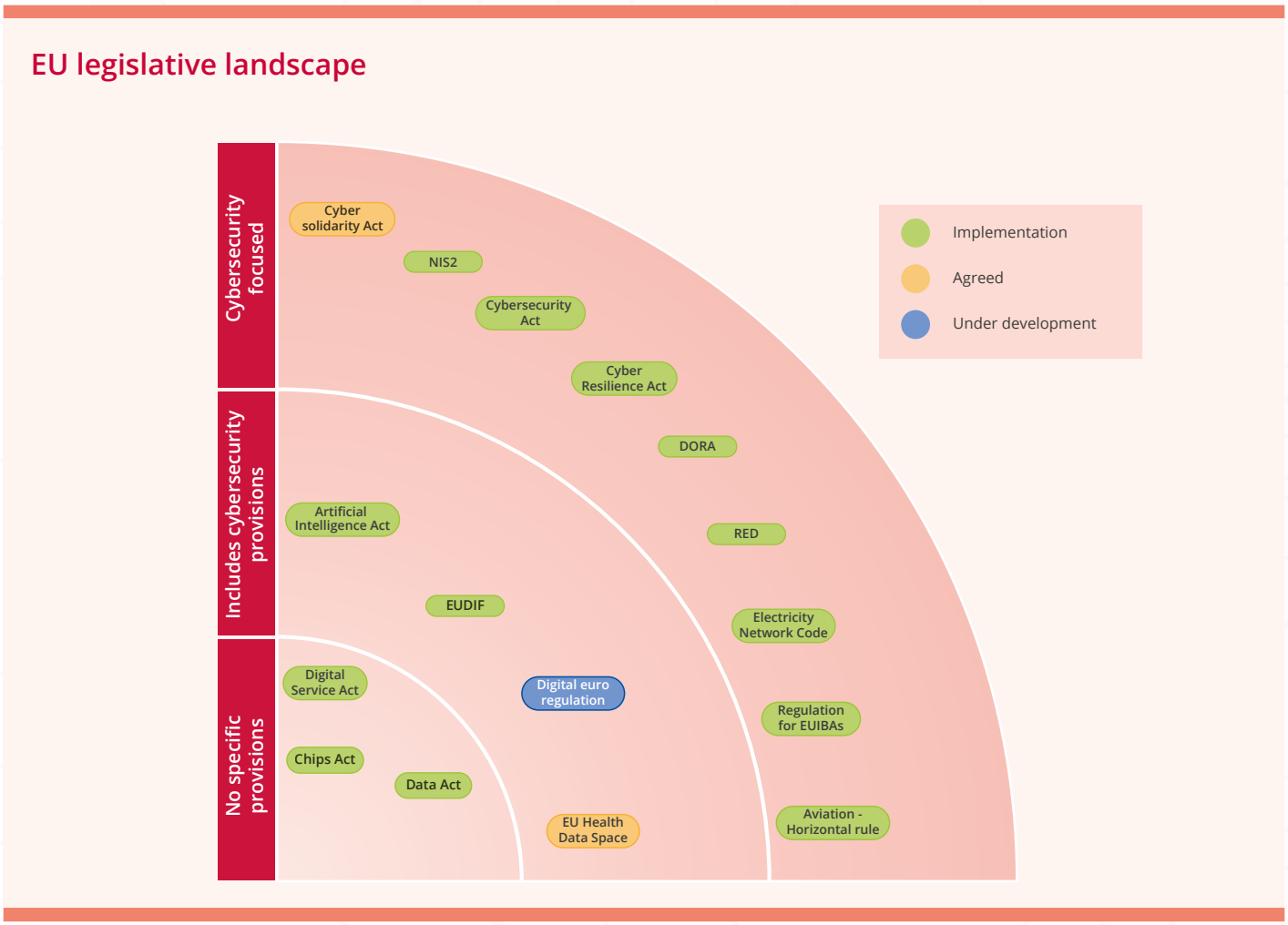
In the recent past, several legislative developments have taken place. After the entry into force of the Directive (EU) 2016/1148 (**NIS Directive**[3]) in 2016 and the **Cybersecurity Act**[4] in 2019, a major policy milestone at EU level was the **EU Cybersecurity Strategy** (published on 16 December 2020)[5]. Several regulatory measures have been taken since then, with important new legislation being put in place to complement the EU cybersecurity framework. More specifically, mention shall be made of the following legislative files.

- Five years after the date of transposition of the NIS Directive, the **new NIS2 Directive** entered into force on 16 January 2023 setting the date for transposition by the Member States on 17 October 2024. The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU by imposing legal obligations on entities across 18 sectors of the economy, including in terms of security requirements and the notification of incidents. It also requires Member States to increase preparedness with, for instance, extended prerogatives and missions for Computer Security Incident Response Teams (CSIRTs) and competent authorities. The NIS2 Directive also promotes cooperation among all Member States by continuing and strengthening the Cooperation Group set up originally under the NIS Directive to support and facilitate strategic cooperation and the exchange of information among Member States. It also institutionalises the EU-CyCLONe network, aimed at improving preparedness for and the coordinated management of large- scale cybersecurity incidents and crises at the operational level and to ensure the regular exchange of relevant information among Member States and EUIBAs.
- The **Cyber Resilience Act** (CRA)[6] was adopted on 23 October 2024. The CRA introduces common cybersecurity requirements for products with digital elements, hardware and software, with the aim of minimising product vulnerabilities and ensuring that cybersecurity is taken seriously both at the design and production phases and that vulnerability management is guaranteed across the support period for such products. Manufacturers will have to apply the rules 36 months after their entry into force. Reporting obligations regarding actively exploited vulnerabilities and severe cybersecurity incidents are also introduced, applicable 21 months after the entry into force of the Act.
- The **Cyber Solidarity Act** (CSOA)[7] is expected to enter into force in early 2025. The CSOA lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. It introduces three main pillars to strengthen solidarity at Union level to better detect, prepare for and respond to significant or large-scale cybersecurity incidents, comprising the European Cybersecurity Alert System (pan-European Network of Cyber Hubs), the Cybersecurity Emergency Mechanism and the European Cybersecurity Incident Review Mechanism.
- The **amendment to the Cybersecurity Act** (CSA amendment)[8] is expected to enter into force by the end of 2024. The proposed targeted amendment aims to enable, by means of implementing acts by the Commission, the adoption of European cybersecurity certification schemes for 'managed security services', in addition to information and communications technology (ICT) products, ICT services and ICT processes, which are already covered under the Cybersecurity Act.
- The **Regulation regarding measures for a high common level of cybersecurity at EU Institutions, Bodies and Agencies of the Union** (EUIBAs)[9] was adopted in 2023 and entered into force on 7 January 2024.
- Commission Implementing Regulation (EU) 2024/482 which lays down rules for the application of the Cybersecurity Act as regards the adoption of the **European Common Criteria-based cybersecurity certification scheme** (EUCC)[10] entered into force in February 2024 and will be applicable as of 27 February 2025.

- A number of **sector-specific cybersecurity initiatives**, such as:
  - Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)[11] entered into force on 16 January 2023;
  - Commission Delegated Regulation (EU) 2022/1645[12] and Commission Implementing Regulation (EU) 2023/203[13] were adopted in 2022 in the aviation sector;
  - The Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)[14] was adopted on 11 March 2024;
  - The new European Digital Identity Framework[15] amending Regulation (EU) No 910/2014[16] entered into force in May 2024;
  - The European Health Data Space (EHDS)[17] Regulation is in the final stages of the adoption process.
- Other **recent Union legislation relevant to the cybersecurity realm** include among others the Artificial Intelligence Act (AIA)[18], Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act - DMA)[19], Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act - DSA)[20], Regulation (EU) 2023/178 (Chips Act)[21] and Regulation (EU) 2023/2854 (Data Act)[22].

These policy files include legislative initiatives that explicitly focus on cybersecurity, such as NIS2 and the CRA, legislative initiatives that include cybersecurity provisions as part of a broader context, such as the AIA and the EHDS, and legislative initiatives that, despite not including specific cybersecurity provisions, are relevant from a cybersecurity standpoint, such as the Chips Act.

**Figure 1:** Overview of EU legislative landscape during the reporting period



## 1.2 UNION-LEVEL RISK ASSESSMENT

For the purpose of this report, the union-level risk assessment focuses on identifying and displaying the Union's exposure in the cyber threat landscape. During the reporting period, the EU experienced a surge in cyber threats, fuelled by factors such as the fast pace of digitisation and the ever-increasing interconnectivity of our society and economy. The cybersecurity threat landscape has become and continues to be significantly more complex and widespread[23]. The geopolitical landscape heavily influences the goals and tactics employed by state and non-state threat actors. Malicious cyber activity has become a clear component of wider hybrid threats, such as disinformation and physical acts of sabotage and violence, seeking to undermine and destabilise EU society, democracy and values. The ongoing Russian war of aggression against Ukraine initiated in February 2022 and the escalated Israel-Palestine conflict since October 2023 continued to impact the cybersecurity realm, in particular in connection with rising threats of Foreign Information Manipulation and Interference (FIMI)[24] and hacktivism. Similarly, major events taking place at the national or European levels provided the motivation for increased hacktivist activity (for example, the European Elections)[25].

In addition, the fading out of the COVID-19 pandemic did not result in a decrease in the use of digital services. On the contrary, a continued demand for the use of digital devices from businesses and citizens was seen in 2023[26]. Moreover, the rise of AI-powered technologies and tools continued to have an impact on societies across the EU[27].

EU MSs continued to be targeted by cybercriminals, state-aligned threat groups and hacktivists who displayed continuous evolution and the updating of their tactics, techniques and procedures (TTPs) in conducting campaigns against governments, organisations and civil society. Furthermore, the systems of EU MSs as well as Union entities continue to be exposed to the exploitation of known and unknown vulnerabilities.

In light of the observations and findings concerning the cyber threat landscape, the cyber threat level to the EU during the reporting period was assessed as **substantial**[28], meaning that it is likely entities are being directly targeted by threat actors or could be exposed to breaches using recent discovered vulnerabilities, while serious disruptions of essential and important entities or EUIBAs is considered a realistic possibility. The substantial severity of the threat is also based on the intent and capability of the threat actors. While the threat actors we tracked demonstrated the intent to generate high-scale cybersecurity incidents in Europe, only some of them had previously displayed the capabilities needed to cause them.

## 1.3 EU CYBER THREAT LANDSCAPE

This section provides a comprehensive overview of the evolving threat landscape in the EU, based on available insights and our understanding of current challenges and emerging trends. According to the ENISA Threat Landscape 2024 report[29], from late 2023 to mid-2024 there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences[30].

In Figure 2, it can be seen[31] that the category of Denial-of-Service attacks (DoS/DDoS/RDoS) and ransomware remained the most reported forms of attack and accounted for more than half of the events observed followed by threats against data, for example data breaches or data leaks.

- As geopolitical and economic tensions grow, cyber warfare escalates with espionage, sabotage, and disinformation campaigns becoming key tools for nations to manipulate events and secure a strategic advantage.
- According to ENISA's analysis of cybersecurity incidents and cyber threats[33], **cyberespionage** campaigns targeting EU MSs and EUIBAs are continuous and remain a persistent and severe threat, despite limited public reporting. Russia-nexus and China-nexus[34] threat groups remain prominent threats. In particular, Russia-nexus groups continue focusing on Ukrainian targets[35], while updating their infrastructure to conduct cyberespionage campaigns against EU countries and institutions and advanced cyber offensive campaigns against technology providers, gaining access to high value targets. The European Parliamentary elections were seen to be a target with information operations aligned with Russian and Chinese interests aiming at influencing the civilian population[36], but did not include any notable or disruptive cyberattacks.
- According to a recent analysis[37] of **Foreign Information Manipulation and Interference** (FIMI) cases detected between December 2022 and the end November 2023, it was noted that EU-based organisations are a common target of such activities.

  Threat actors rely on the repetitiveness of their actions, as individual incidents may seem small on their own and may not be visible; however, these subtle attacks can gain power through persistence and repetition. Also, many hacking campaigns by state-nexus threat actors are using AI to create fake content or to develop new ways to spread misinformation. According to the recent ENISA Threat Landscape 2024 report[38], information manipulation continues to be a key element of the Russian war of aggression against Ukraine, although an effort to further localise content and at the same time to globalise its presence is observed. According to the ENISA foresight study[39] on

cybersecurity threats for 2030, the spotlight is on the growing relevance of cybersecurity in elections and the role of disinformation with AI content.

- In the context of the **cybercrime** ecosystem, **ransomware** remains among the most impactful threats for EU Member States, with a shift from encryption to data exfiltration and with small and medium-sized enterprises becoming a more attractive target for cybercriminals, while the double extortion tactic has become the norm for well-established ransomware groups[40].

  Cybercriminals continue to use **social engineering** techniques, such as phishing e-mails with malicious links or social media, to trick people into revealing their credentials, while they are also using AI to create fake content, such as phishing e-mails and deepfakes[41]. A concerning trend that has gained momentum in recent years is the rise of **hacker-for-hire** services that contribute to the professionalisation of the cybercrime market, but also provide services to state-nexus actors. High-profile arrests[42,43] and successful take-downs show that there is an ongoing concerted effort to dismantle criminal networks by law enforcement agencies. In many cases, law enforcement actions have forced criminal groups to reorganise themselves, signalling a downward trend that will likely force cybercriminals to move towards new profitable business models.

**Figure 2:** Breakdown of incidents by threat type (July 2023 to June 2024)[32]

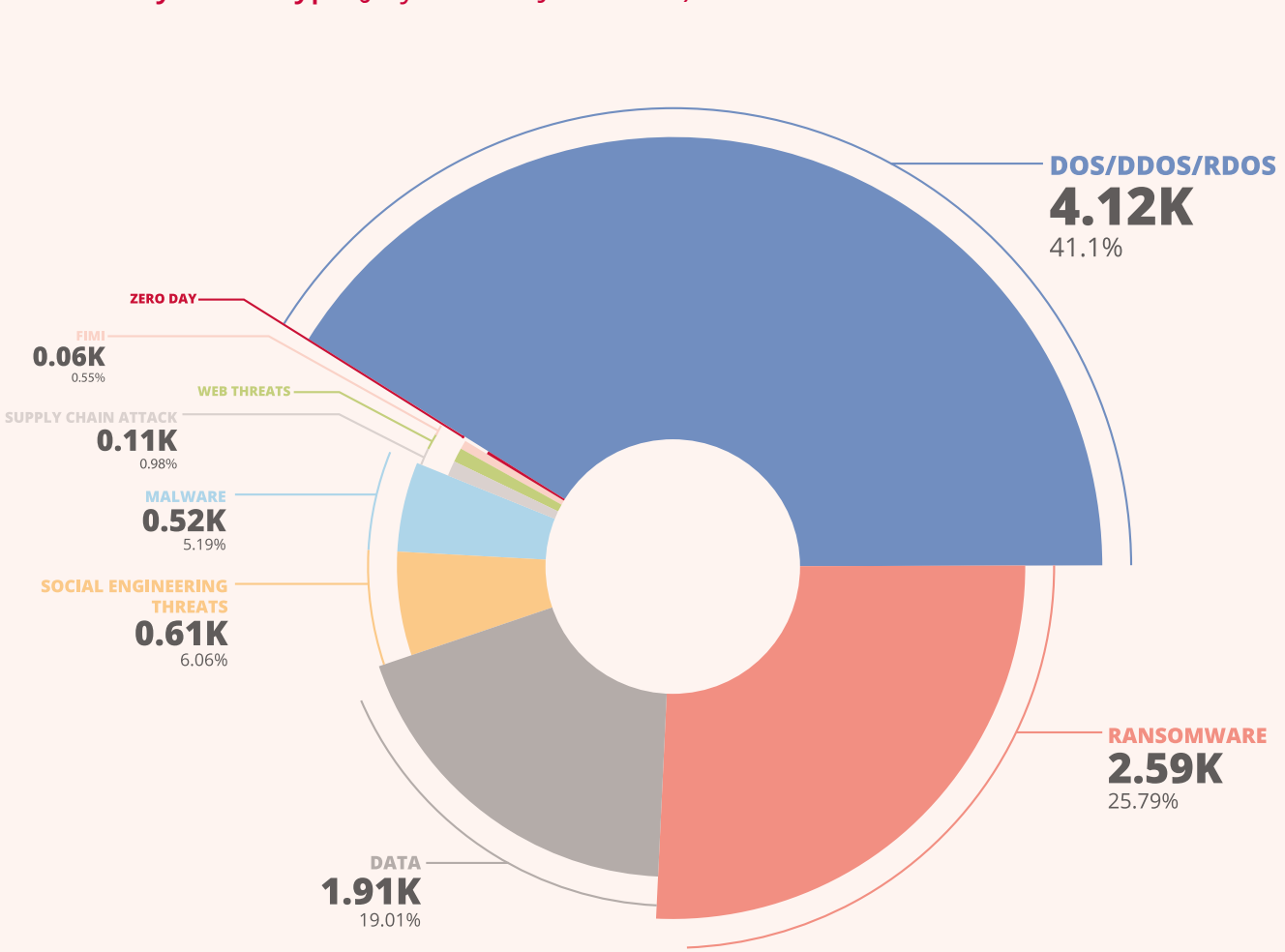
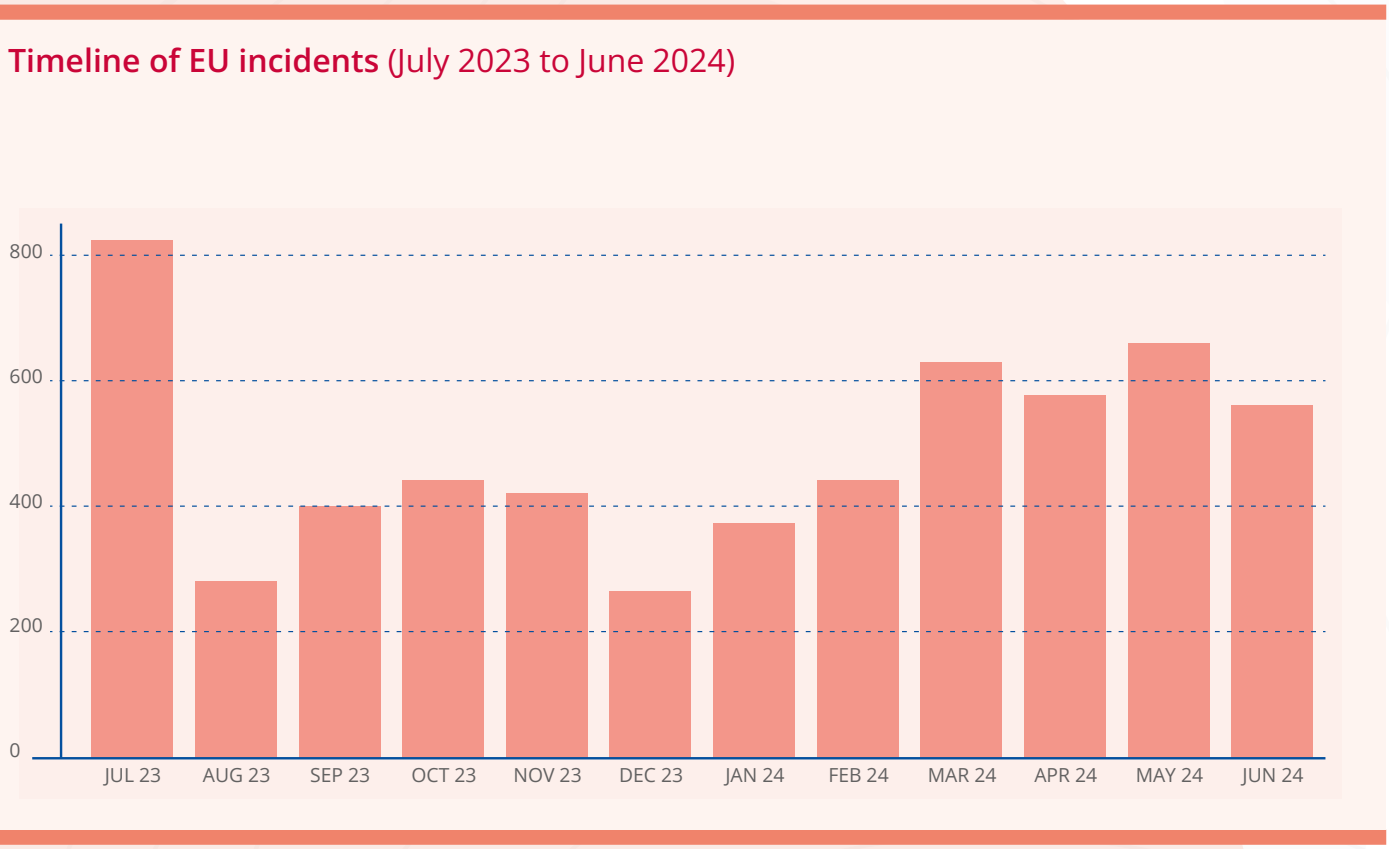


**Figure 3:** Timeline of EU incidents (number of incidents per month) (July 2023 to June 2024)[44]




- Meanwhile, **hacktivist** activity is increasing and becoming more unpredictable. According to the 2023 Internet Organised Crime Threat Assessment[45] by Europol, the ongoing geopolitical crisis has unleashed a wave of disruptive cyberattacks, with the EU MS bearing most of the effect of these malicious activities.

  Hacktivists use common tactics, such as DDoS attacks and website defacements, but also "Fear, Uncertainty, and Doubt" to amplify the impact of their operations. A huge number of Distributed Denial of Service (DDoS) attacks have significantly targeted the public sector across the EU among others.

  Further, hacktivists use ransomware and wipers[46] and rely on data theft[47]. A notable trend is the overlap between state-nexus actors and supposed hacktivists. Pro-Russian hacktivist activity against European targets has increased throughout the reporting period, while its operational impact remains limited and seems mainly aimed to attract attention or support propaganda campaigns. The vast majority of hacktivist attacks continue to be driven by the Ukrainian conflict or perceived anti-Russian stances, with occasional instances of pro- Palestinian hacktivist groups potentially targeting EU Member States. Threat actors continue to make use of their DDoS tools to further amplify their targeting. While currently the alliances among hacktivist groups appear to have minimal impact on their reach, the convergence of two or more prevailing groups could potentially generate impactful incidents.

# *Hacktivist activity is increasing and becoming more unpredictable*

Hacktivists use common tactics, such as DDoS attacks and website defacements, but also “Fear, Uncertainty, and Doubt” to amplify the impact of their operations.

**A notable trend is the overlap between state-nexus actors and supposed hacktivists.**

**Figure 4:** Time series of DDoS incidents (July 2023 to June 2024)[48]

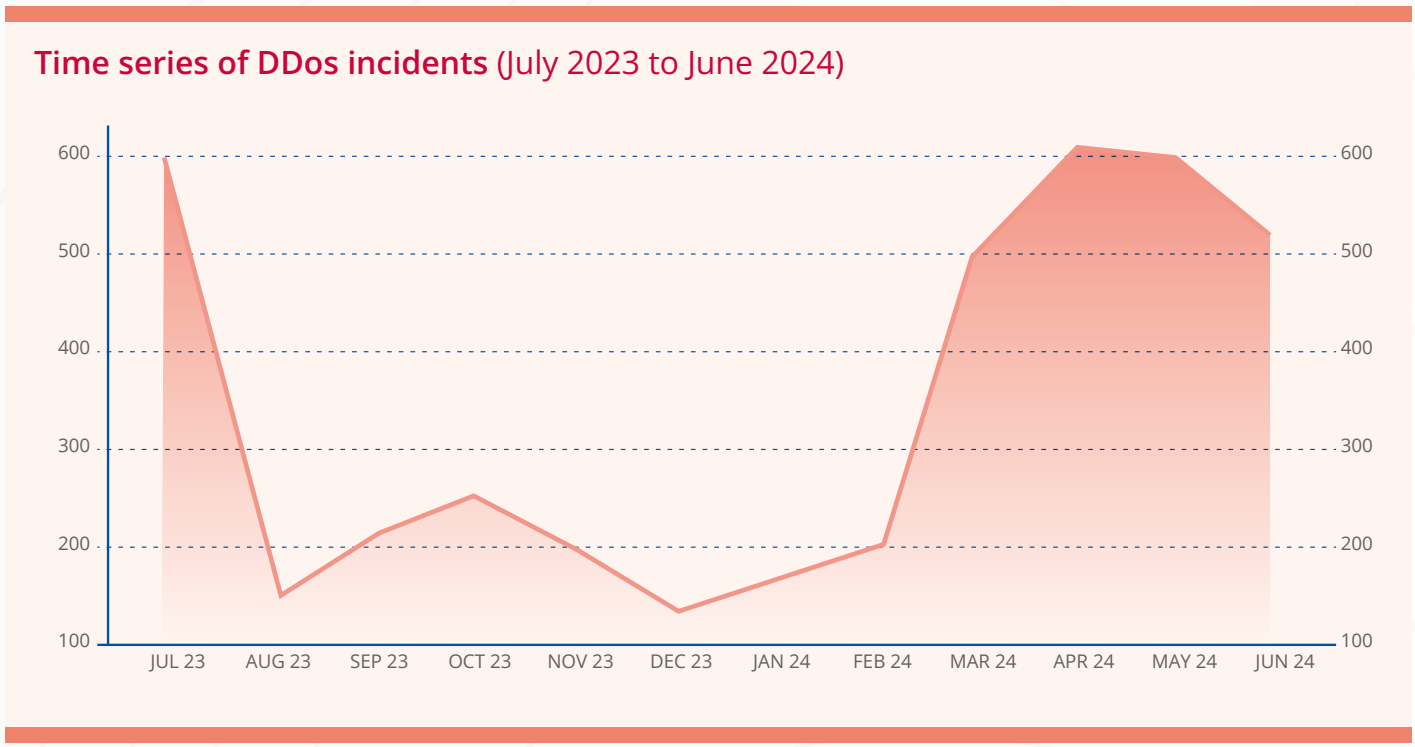
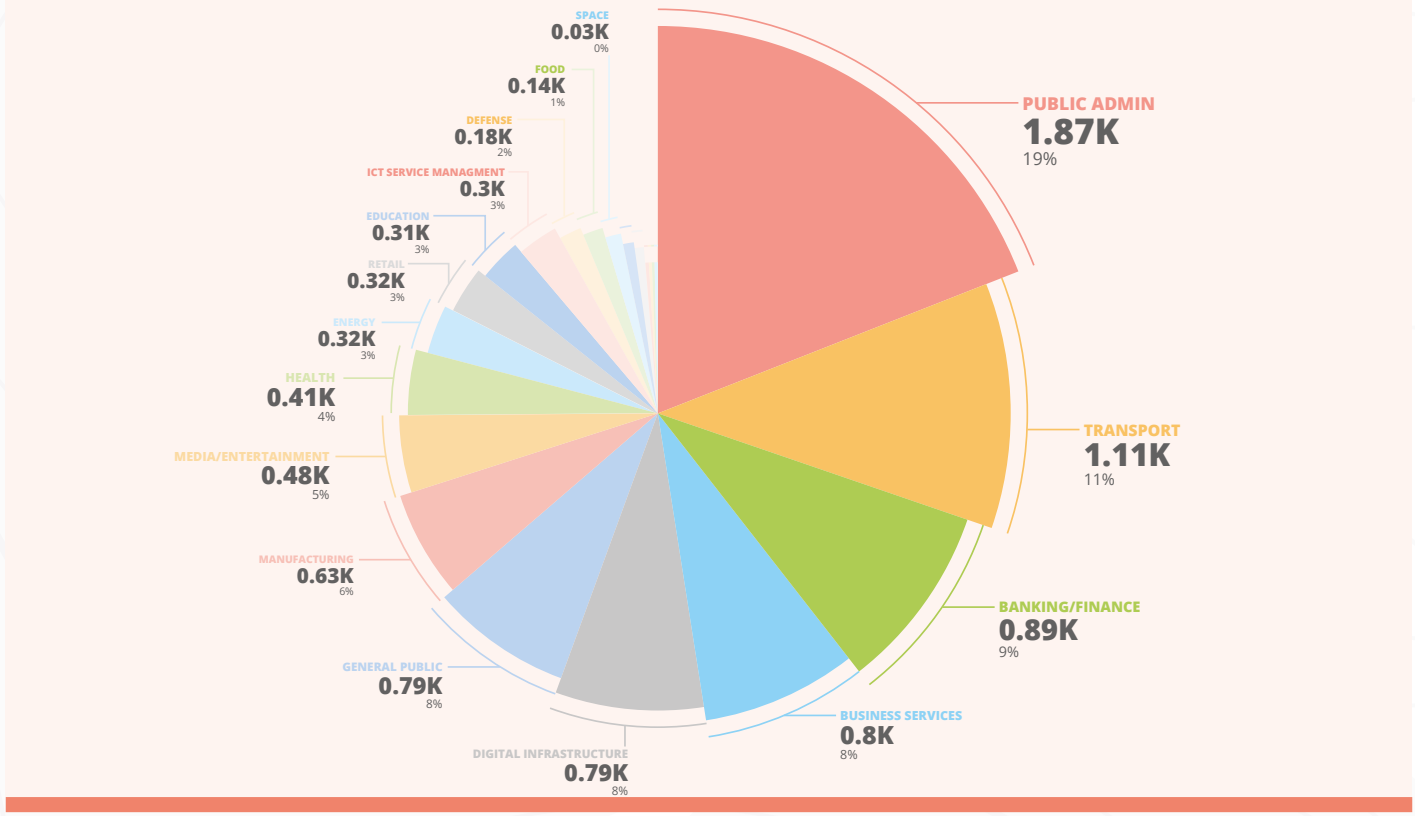



**Figure 5:** Targeted sectors per number of incidents (July 2023 to June 2024)[53]



- **Supply-chain** threats rank highly in the EU, because of their wide reach, their difficulty in detection and the significant potential they have in inducing catastrophic cascading effects. On top of the ever-increasing reliance on outsourced IT services, creating supply chain complexities and cybersecurity challenges, especially for SMEs[49], the alarming rise of sophisticated supply chain attacks demands a multi-pronged approach to fortify defences.
- Finally, while multiple state-nexus threat groups reportedly continue to exploit zero-day **vulnerabilities** in the context of targeted espionage, unpatched vulnerabilities (N-day vulnerabilities) remain a greater risk due to their impact on a wide array of organisations[50].
- The interconnected digital age leaves no sector immune to cyberattacks. According to the ENISA Threat Landscape report 2024[51], a large number of events have been observed (Figure 5) targeting organisations 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 was recorded targeting civil society though not necessarily a particular sector (these are labelled as 'general public') and accounted for 8% of all events observed[52].

**Figure 6:** Review of the ENISA Foresight Cybersecurity Threats for 2030.

- **Giving an outlook into the long-term future**, the increased dependencies and the development of new technologies, such as quantum computing and AI, add complexity to the threat landscape and introduce new risks for which further preparedness is needed.

According to an ENISA study[54] that analyses and forecasts emerging cybersecurity threats up to 2030, the spotlight is on the increasing power of non-state actors. More specifically, according to the trends identified, while the perceived prominence of threats such as 'supply chain compromise of software dependencies' and 'advanced disinformation/influence operations campaigns' is expected to decline slightly until 2030, they will still pose significant risk. The 'human error and exploited legacy systems', the 'exploitation of unpatched and out-of-date systems' and the 'physical impact of natural/environmental disruptions on critical digital infrastructure' will gain ground in their level of threat as perceived. Similarly, the risk of 'advanced hybrid threats' linked to interference, social engineering tactics and the dissemination of disinformation are considered to be within the top-ranking ones in, for example, the context of elections. On the other hand, long term perspectives of threats such as 'skill shortages' have intensified. The likelihood that 'AI disrupting or enhancing cyberattacks' will appear has increased, which is not surprising given the wide coverage of emerging AI applications at scale and considerations for the ethical use of newly released and emerging AI models.

Chapter II

# CYBERSECURITY CAPABILITIES AT THE UNION LEVEL

## 2.1 HIGH-LEVEL FINDINGS

In accordance with Art. 18.3 of the NIS2 Directive, ENISA has developed a set of quantitative and qualitative indicators (combined in a framework hereby referred to as the "EU Cybersecurity Index") to support the aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union. The framework describes the cybersecurity posture of the EU in selected areas, including the ability of society and the private sector to recognise threats and prevent incidents, the state of policy development and implementation, and the ability to carry out operations to ensure resilience.

By combining the value of quantitative and qualitative indicators, the Index results in an aggregated assessment of the EU as a whole and on specific aspects[55]. Based on the data collected in 2024, the overall value of the Index is 62.65 (on a scale from 0 to 100 points). It is noted that the average deviation of the scores of Member States from the EU average is 3.76, signalling an overall convergence across the Union with regards to the set of indicators as assessed, with some countries lagging slightly behind (with the minimum deviation being -13.18 points).

**Figure 7:** EU Cybersecurity Index 2024 – Source: ENISA

**There seems to be convergence among MSs in the domains where the EU average is the highest.** In general, the indicators with the lowest average deviation from the index among MSs (below 3 index points) largely correspond to the indicators with the highest average values (90 points or above).

**MSs seem to diverge especially in domains related to policy implementation, in particular with regards to vulnerability disclosure and supervisory measures for essential and important entities, as well as R&D and education.** In these domains, the average deviation of related indicators is among the highest (25 points or more) and there is a big difference between the countries deviating the most and the least from the EU average. As regards to vulnerability disclosure and supervisory measures, this is due to the ongoing implementation of relevant legislation. As regards to R&D and education, this seems to indicate that different MSs perceive the importance of the topic differently. Sections 3.4.1 on Vulnerability Handling and Disclosure and 3.1.2 on Identification and Supervision give more detailed information on different stages of implementation in MSs. The info box on R&DI and section 2.3 on skills give more contextual information to mentioned topics.

**R&D and innovation are indeed topics where EU average values hide great discrepancies among MSs.** The indicators measuring the share of EU funding for cybersecurity R&D and, as mentioned above, on the coverage and implementation of cybersecurity in national R&D policies and initiatives show high values for the maximum and minimum deviations from the EU index average.

**In the field of cyber hygiene, the secure internet use of citizens showed one of the highest results.** This indicator has an EU average score of 93.29 out of 100 and a low average deviation amongst MSs. This means that, across all MSs, internet users have changed the way they use the internet due to security concerns. Section 2.4 on Cybersecurity Awareness and Cyber-Hygiene puts this finding into the context of people's confidence into their ability to protect themselves.

**The EU has a high average score in relation to enterprises that have not suffered cybersecurity incidents leading to the disclosure of confidential data or destruction and corruption of data.** The related indicators have an average EU value above 90 out of 100 and a low average deviation amongst MSs[56]. It is important to note though that, in general, enterprises, and especially SMEs, are reluctant to admit having been a victim of an incident. Section 3.1.4 offers a more in-depth analysis on incident reporting.

**There is room for improvement regarding cybersecurity investments performed by Operators of Essential Services (OESs) and Digital Services Providers (DSPs) regulated under the NIS1 Directive[57].** The EU average for the related indicator is low (7.14) and the average deviation is low (0,54), meaning that this issue seems to be wide-spread across the EU. A more detailed analysis on the Cybersecurity Capabilities of Critical sectors is section 2.3.

Another area needing improvement is **cybersecurity governance within organisations**. In particular, the EU average score for enterprises performing a **cybersecurity risk assessment** is 32.01 out of 100. Section 3.1.3. puts this finding in the broader context of the national Cybersecurity Risk Management measures.

**The maturity of CSIRTsis also an aspect where more action would be needed.** The EU average score for the related indicator measuring the alignment of CSIRTs with internationally recognised practices[58], is low (10.31 out of 100) and the average deviation from this value is 10.58.This indicates that low maturity, in terms of certification, is a relatively common characteristic among MSs. On the positive side, CSIRTs seem to be well-integrated in international networks, such as Trusted Introducer and FIRST. Section 3.2.2 explains and builds on the role of CSIRTs in crisis management.

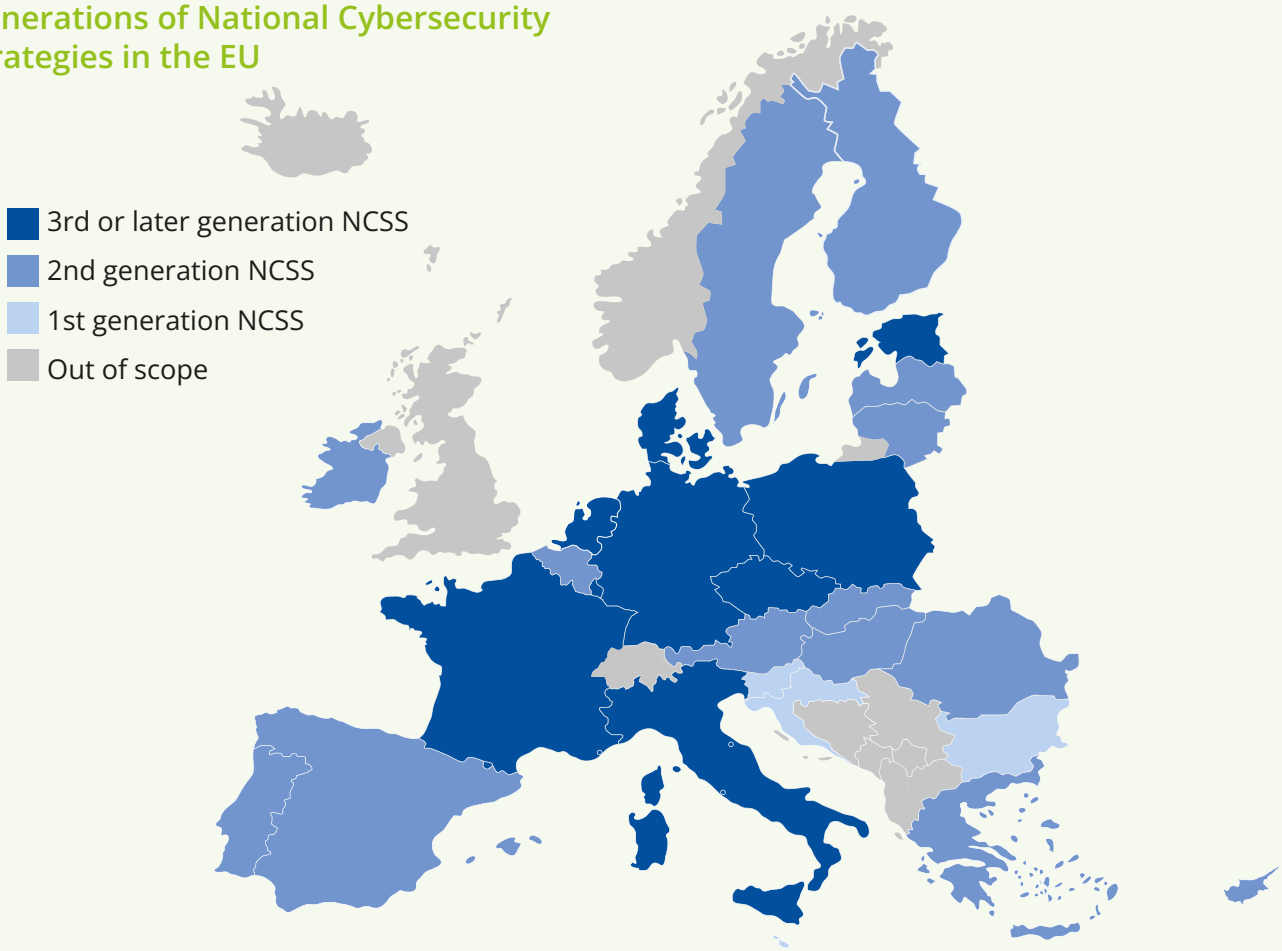
## 2.2 NATIONAL CAPABILITIES: ALIGNMENT OF NATIONAL CYBERSECURITY STRATEGIES

National cybersecurity strategies (NCSS) are documents setting a country's long-term policy vision for cybersecurity. NIS2 mandates that each MS adopts "a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity [...][59].

Since 2017 **all MSs have a national cybersecurity strategy** which, in some cases, were also updated in later years[60]. The MSs have different degrees of expertise in drafting strategies, ranging from some being at the third (or more) generation of their strategy to others being at their first generation.

**Figure 8:** NCSS generation in the EU (2023) – Source: ENISA, A governance framework for National Cybersecurity Strategies[61]

### Generations of National Cybersecurity Strategies in the EU




Out of the 27 Member States:

- 9 Member States have a 3rd or later generation NCSS.
- 14 Member States have a 2nd generation NCSS.
- 4 Member States are at their first NCSS.

While it is normal that MSs can have varying priorities due to their national contexts, alignment of objectives indicates that national efforts are addressed in the same direction, thus facilitating complementarity and creating a potential for economies of scale.

Looking at a pre-identified set of strategic objectives[62], national strategies are overall aligned, as most objectives are shared across the great majority of MSs[63].

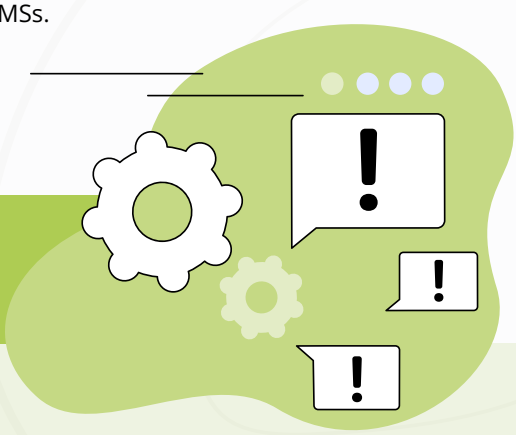
## The most common objectives in National Cybersecurity Strategies are:

**National strategies are aligned overall, with most objectives shared across the great majority of MSs. The least recurrent objective concerns the cybersecurity of the supply chain included by only half of MSs in their strategies.** Supply chain security has become an increasingly urgent matter in the few last years due to the discovery of impactful vulnerabilities (e.g. Log4j[64]) and the geopolitical weaponisation of supply chains[65]. The relatively low take-up of a related objective might reflect a certain difficulty in rapidly adapting strategies to a changing context. This might change from sector to sector; for example, in the context of the EU Toolbox on 5G Cybersecurity[66] for the protection of 5G networks, measures have been taken at the national level to exclude high-risk vendors.

**Objectives in national strategies are generally matched by formal action plans that are then implemented. However, there is a group of MSs that have put in place the necessary policy framework but are lagging behind in the definition of action plans.**

In order to be meaningful, the coverage of cybersecurity objectives is expected to be matched by formal action plans that are then implemented. Generally, it is the case that almost all most common objectives (10 out of 12) are complemented by an action plan in the majority of the MSs (80% or more) that included those objectives in their national strategies. However, for **half of the most common objectives it can be observed that the share of MSs that have implemented their action plans decreases** (between 67 and 79%). This suggests that there is a group of MSs that have put in place the necessary policy framework but are lagging behind in the implementation of action plans.

The eventual implementation of the **Peer Review** process introduced in Art.19 of NIS2 is expected to further enhance cybersecurity capabilities at national level through the sharing of good practices and the development of mutual trust among MSs.



## Info box

### R&D&I in national cybersecurity strategies

Research, development and innovation (R&D&I) are generally regarded as fundamental forward-looking activities to ensure a country's technological and economic competitive edge. This holds also for cybersecurity because of the fast-moving nature of related technologies, as well as for its role in the security and perceived trustworthiness of the digital environment. Cybersecurity R&D&I is generally recognised as important and features as a dedicated objective in national strategies; the great majority of MSs (23) include a dedicated objective in their national strategies. The level of implementation is mature in about two-thirds of the countries (17) that implement that objective with, for example, a dedicated body overseeing cybersecurity R&D, funding programmes and joint public-private investments as well as the establishment of local start-up ecosystems and other networking channels. Less than one-third (six MSs), however, has put in place mechanisms to detect the need for updates or the inclusion of new measures. While the difficulty in updating programmatic documents is acknowledged, R&D&I is an area in which delayed implementation or delayed updates might lead to significant consequences.

### What about the cybersecurity of institutions, bodies, offices and agencies of the European Union?

In the digital age, information and communication technology is a cornerstone of an open, efficient and independent European administration. Evolving technology and the increased complexity and interconnectedness of digital systems amplify cybersecurity risks, making EU institutions, bodies, offices and agencies ('Union entities') more vulnerable to cyber threats and incidents which pose a threat to their business continuity and capacity to make their data secure. In December 2023, Regulation (EU) 2023/2841 that lays down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union was adopted[67]. Among others, the regulation mandates that each entity establish, by 8 April 2025, a framework for internal cybersecurity risk- management, governance and control to be overseen by and under the responsibility of the Union entity's highest level of management. Also, the regulation foresees the creation of an Interinstitutional Cybersecurity Board, adopting a multiannual strategy on raising the level of cybersecurity in Union entities.

## 2.3 PRIVATE SECTOR CAPABILITIES: CYBERSECURITY CAPABILITIES OF CRITICAL SECTORS

The NIS1 and NIS2 Directives cover a wide range of different sectors, each with their own criticality and maturity, and with their own cybersecurity needs. To allow for an assessment of the capabilities, and to understand the needs of each sector, ENISA developed a **methodology** to assess, on an annual basis, **the cybersecurity maturity** and **criticality** of each NIS sector from a Union-wide perspective[68]. Through a combination of qualitative and quantitative indicators, each sector is evaluated across four critical and five maturity dimensions, scoring them from 1 to 10[69].

| Criticality Dimensions | Maturity Dimensions |
|---|---|
| 1. **Dependency on ICT:** Higher dependency means increased vulnerability**.**<br>2. **Time-Criticality:** Quick impact requires rapid response**.**<br>3. **Economic Impact:** Understanding economic consequences helps prioritise protection**.**<br>4. **Health and Safety Impact:** Protecting human lives is paramount**.** | 1. **Policy Framework and Guidance**: Strong policies are foundational.<br>2. **Risk Management and Good Practices:** Effective risk management enhances resilience.<br>3. **Collaboration and Information Sharing**: Key to staying ahead of threats.<br>4. **Operational Preparedness:** Ensures swift response to incidents.<br>5. **Security of ICT:** Critical to protect operations from cyber threats. |

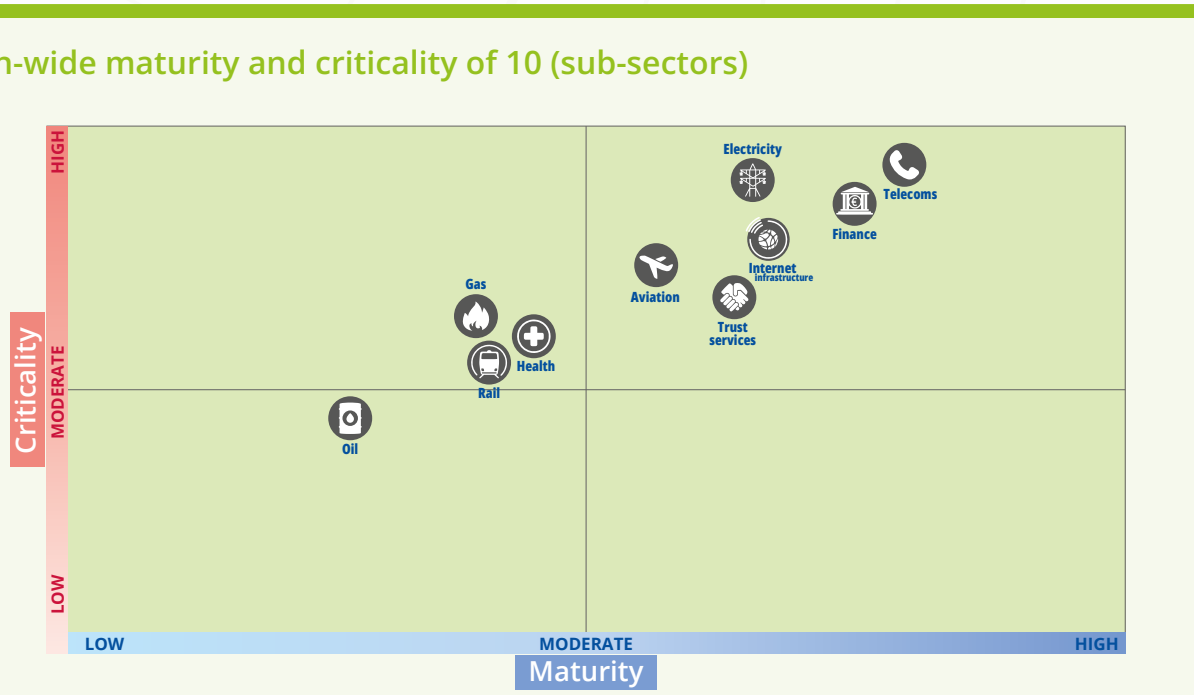
In 2023, ENISA conducted this assessment for the first time as a **pilot** initiative[70]. This first assessment focused on a limited number of sectors and subsectors (or types of entities within a sector)[71] to ensure a manageable and effective evaluation process, including:

- **Digital Infrastructure** sector, covering the following types of entities:
  - **Providers of public electronic communications networks** in the Digital Infrastructure sector (hereafter called **Telecoms** subsector)
  - **Internet Exchange Point providers, Content delivery network providers, TLD name registries, DNS service providers** (hereafter called **Internet infrastructures** subsector)
  - **Trust Service Providers** (hereafter called **Trust Services** subsector)
- **Energy** – covering subsectors **Electricity**, **Gas** and **Oil**
- **Banking** and **Financial Market Infrastructures** sectors (hereafter called **Finance**)
- **Health** sector
- **Transport** sector – covering two subsectors **Aviation (Air)**, and **Rail**

Their overall Union-wide sectorial criticality and maturity scores are shown in Figure 9. **MSs and their national authorities may need to prioritise between the various sectors**, deciding which sectors could receive more focus. This prioritisation will depend on many factors of course, but one factor which could be considered is the relation between the criticality of a (sub)sector and the maturity of a (sub)sector

It is important to mention that all **sectors face heterogeneity in terms of entity size and criticality**, making it challenging for national authorities to supervise and enforce uniform security requirements.

**Figure 9:** Union-wide maturity and criticality of 10 (sub)sectors




## Key sectors and subsectors with High Maturity and Criticality: Telecoms, Electricity, and Finance

The telecommunications, electricity and finance (sub) sectors form the backbone of modern society, boasting the highest criticality scores due to their essential role in maintaining daily life and economic stability. Their failure would immediately and profoundly disrupt our daily lives and economic activities. Additionally, these sectors show the highest maturity levels in cybersecurity, thanks to **strong regulatory frameworks**, **effective supervisory authorities**, and **advanced risk management and operational preparedness**. Consequently, their cybersecurity practices serve as benchmarks for other sectors.

In a majority of these 'big three' sectoral entities (80%), leaders are directly involved in approving cybersecurity risk management measures. **There is a very strong correlation between management involvement in cybersecurity and an organisation's cyber risk management maturity and incident detection and response capabilities**. Organisations with leadership active in cybersecurity are more than twice as likely to score above the basic level in both risk management and incident detection and response[72].

However, there is diversity among entities within these sectors. For example, leadership training in cybersecurity is highest in banking (59%) but lowest in financial market infrastructures (30%). Similarly, the banking sector has the highest information security spending per annum (€2.0million), whereas the financial market infrastructures sector has one of the lowest IS (Information Security) spending per annum (€0.3m).

## Emerging subsectors in Criticality: Internet Infrastructure

As our world becomes more digital, Internet Infrastructure is becoming increasingly critical. Its stability is crucial for the functioning of other (sub)sectors. However, while its criticality is nearing that of the big three, its maturity still needs improvement.

Entities in these NIS2 sub-sectors **are very aware of cyber risks** and have **developed good practices in cyber risk management**. However, the level of cyber experience among entities is highly divergent, which contributes to discrepancies. Additionally, both at the national and EU levels, the **understanding and follow-up of cyber risks concerning these sub-sectors are limited**. This limited understanding may contribute to the sector's reported deficiencies in incident detection, response capabilities and overall capabilities in the management of cyber risk.

Similarly, at the level of entities, **operational preparedness is quite high**. Most of the entities, such as the Internet exchange points (IXPs) and the Content delivery networks (CDNs), are dealing with cyberattacks on a daily basis. However, the **lack of information sharing and collaboration between the entities and authorities** also complicates operational collaboration in the event of a crisis. Enhancing these areas is essential for maintaining the security and stability of our digital ecosystem.

## Moderate Criticality and Maturity: Health, Railway, and Gas

Sectors and subsectors such as health, railway and gas have moderate to high criticality scores. For instance, hospitals are primarily targeted by cyber criminals which may or may not result in patient data being leaked. However, these effects related to confidentiality are expected to be manageable. Incidents affecting the availability of health services may in fact put health or safety at risk. According to the ENISA Threat Landscape 2023 report, the health sector is one of three sectors facing the highest number of cybersecurity incidents. Moreover, according to available data on the threat landscape, even severely disruptive incidents affecting the health sector are typically isolated events with no cross-sectorial impact (in contrast to, for example, an incident affecting the Electricity sub-sector).

Similarly, an incident in the railway sub-sector would have an effect at a national level but is not likely to have a spill over impact. The health sector is becoming increasingly dependent on ICT for a range of applications, from medical instruments to patient databases, whereas the gas sub-sector uses ICT tools and systems to a moderate extent in its operations and is not yet heavily dependent on them.

These three (sub)sectors have moderate maturity levels, facing **challenges in securing legacy systems and operational technology (OT)**. Railway and Health entities manage many legacy or obsolete systems which are difficult or even impossible to upgrade in order to implement cybersecurity measures. The respective entities are **reliant on their suppliers**, ICT service providers and other third parties for system updates, patch management and lifecycle management. Furthermore, the **health sector's performance in ensuring the security of the ICT products and processes it uses is rather inadequate** due to a huge variety of health entities, devices and products.

Interestingly, both Health and Rail are among the top investors in IT spending, with the health sector operators investing annually 64 million EUR and the railway subsector 101 million EUR. Addressing the above-mentioned challenges and leveraging their significant IT investments are crucial steps toward enhancing cybersecurity in these vital sectors.

## Low Maturity: Oil sector

The oil sub-sector, while less critical than others due to its lower dependency on ICT and less time-sensitive nature of incidents, shows the lowest maturity in cybersecurity practices. The oil sub-sector is still in the very early days of its digitalisation and journey to maturity in cybersecurity. Significant improvements are needed to elevate the sector's cybersecurity posture and ensure it does not become a weak link in our critical infrastructure.

The Cyber Emergency Mechanism established with the CSOA includes preparedness actions such as coordinated preparedness testing of entities operating in highly critical sectors and is supported from the Digital Europe Programme and managed by the European Cybersecurity Competence Centre. The Commission, after consulting ENISA and the NIS Cooperation Group, could regularly identify relevant sectors or subsectors from the Sectors of High Criticality listed in Annex I of the NIS2 directive, from which entities may be subject to coordinated preparedness testing at EU level[73].

## 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.*

**To achieve this recommendation:**

- A harmonised approach for collecting sector-relevant data could be developed. MSs are encouraged to assess and monitor the maturity and criticality of sectors at the national level. Additional indicators may cover incidents, investments and cybersecurity practices.
- The role of NIS2 as a horizontal framework to improve the level of cybersecurity maturity of sectors in scope should be preserved.
- The EU MSs, with the support of the European Commission and ENISA, could consider offering self-assessments to the entities which fall within the scope of the NIS2 Directive, in addition to other measures such as stress tests.
- The EU is encouraged to capitalise on ENISA's technical expertise in cybersecurity to increase the preparedness and resilience of a sector's cybersecurity and is especially advised to seek ENISA's technical evaluation of any policy initiative that could have an impact on the preparedness and resilience of a sector's cybersecurity.
- A national risk assessment of selected sectors of our economy and society following an all-hazards approach would provide a more granular assessment at national level. This would allow for more information to be introduced in Union-wide risk assessments of specific sectors.
- ENISA could assist EU MSs to assess the cybersecurity of entities falling within the scope of the NIS2 Directive in their jurisdiction, e.g. by providing information or supporting the sharing of good practices and the development of common assessment frameworks.

## 2.4 SOCIETAL CAPABILITIES: CYBERSECURITY AWARENESS AND CYBER-HYGIENE OF EU CITIZENS

The fast pace of digital transition and the formation of new ways to exercise and enjoy fundamental rights and freedoms showcase the importance of strengthening the cybersecurity awareness and digital skills of citizens, a prerequisite for safe operations in this new environment.

Strong societal cybersecurity capabilities are crucial, as they directly impact how vulnerable EU citizens are to cyberattacks in their daily lives. According to the ENISA Threat Landscape 2024 report[23], 8% of the observed incidents during the reporting period targeted civil society, i.e. the general public, with social engineering, data breaches and information manipulation campaigns.

Overall, a population with a high level of awareness and solid cyber hygiene practices is more resilient against cyber threats. This creates a safer and more secure digital environment for everyone, fostering economic growth and empowering individuals to fully participate in the digital age.

**Half of EU citizens lack the digital skills needed to fully participate in society, hindering their access to online services.**

- According to Eurostat, 46% of Europeans[74] (2021) do not possess basic digital skills and are thus not confident when performing activities online and with digital devices nor can they gain the full benefits of digital technologies. This observation is highlighted in the Digital Decade Cardinal Points[75], as half of EU citizens are lacking the skills needed to access the opportunities offered online to, for instance, obtain information from public authorities, use online banking, shop online or other activities related to the Internet or software used for work, learning and participating in society.

A fair digital future requires ensuring everyone has the digital skills needed to embark on their journey of transformation. **An analysis of different socio-demographic groups at the EU level shows that the level of digital skills is better among young people compared to older age groups. In addition, although the digital gender gap is shrinking, there is still a need to promote relevant initiatives to address it.**

- The Digital Skills Dimension of the Digital Economy and Society Index[76] indicated that only 35% of EU citizens aged 55-74 and 29% of retired and inactive citizens have at least basic digital skills, compared to more than 70% in young adults or individuals with higher education.
- In addition, the digital divide persists between rural and urban populations. Only 46% of rural residents possess basic digital skills[77] compared to 61% in urban areas.
- While the basic digital skills gap between men and women has decreased, still the difference in percentage terms between men and women with basic skills is 3.4% (2021), a drop from 5.6% (2015)[78].

**People's confidence in their ability to protect themselves from cybercrime has decreased, suggesting that cybersecurity awareness has likely increased among EU citizens.**

- The confidence of EU citizens in their ability to sufficiently protect themselves against cybercrime has decreased to 59% (2020) from 71% (2017)[79]. This could be justified given the fast-paced digitation of services (public and private) and the more complex and sophisticated threat landscape, but at the same time it could signify an increased awareness of cyber risks among the population.
- This finding complements an observation made, based on Eurobarometer data[80], that a high proportion of Internet users among the population (93%) have changed the way they use the Internet due to concerns about security.

**Low awareness about cybercrime and relevant reporting mechanisms among the EU population.**

- According to Eurostat[81], around two-thirds of individuals in the EU manage access to their personal data on the Internet by, for example, reading privacy policy statements before providing personal data, restricting or refusing access to their geographical location, limiting access to their profile or content on social networking sites, refusing to allow the use of personal data for advertising purposes, checking that the website where personal data are provided is secure. Remarkably, though the risks posed to citizens following the digitisation of services has increased the latest years, this share (66%) has remained stable throughout years from 2020 to 2023.
- The share of population (52%) feeling fairly or very well informed about cybercrime has not changed substantially since 2017 (46%)[82].
- In addition, when it comes to citizens' awareness of cybersecurity matters, just over one in five respondents (22%) responded to a Eurobarometer survey that they are aware of the existence of an official channel to report a cybercrime or other illegal online behaviour.

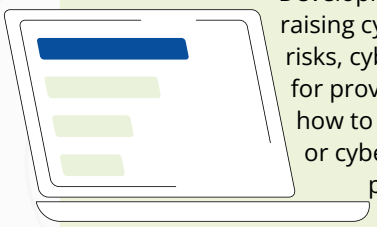
*An analysis of different sociodemographic groups at the EU level shows that the level of digital skills is better among young people compared to older age groups.*

In addition, although the digital gender gap is shrinking, there is still a need to promote relevant initiatives to address it.

**Cybersecurity in higher education: The availability of cybersecurity education programmes varies greatly across EU Member States.**

- When it comes to the development of cybersecurity knowledge in higher education, according to ENISA data[83], more than two-thirds of MSs offer bachelor and master degrees in cybersecurity as an independent discipline in universities (24 MSs), cybersecurity courses and/or specialised curriculum for levels 5 to 8 of the European Qualifications Framework (20 MSs) and actively promote the addition of information security courses in higher education not only for computer science students but also to other professional specialties (21 MSs).
- According to ENISA data shared by MSs on a voluntary basis[84], some MSs have numerous higher education institutions offering cybersecurity programmes, while others have only a few.
- The implementation of funding mechanisms to encourage the uptake of cybersecurity degrees (e.g. scholarships, guaranteed apprenticeship/internship, etc.) seems to vary widely. Sixteen (16) MSs state that they have either not taken any action in this regard or they have only started the process of setting-up funding mechanisms.

## Good practices from Member States



Development of a public website for raising cybersecurity awareness on risks, cyber hygiene practices and for providing clear instructions on how to report a suspicious activity or cybercrime with links to relevant public authorities.

Gamified cybersecurity awareness campaign for young students via a dedicated space with practical tools to facilitate youngsters becoming mindful and alert about relevant threats and risks.

Organisation of several awareness-raising campaigns aiming at 1) developing students' knowledge of finance and cyber security, and 2) allowing them to quickly and easily learn how to recognise cyberattacks and how to avoid them. Also, organisation of a series of educational events, campaigns, conferences and webinars in this regard, as well as TV spots with well-known personalities, to raise awareness.

**Cybersecurity in primary and secondary education: Variations across MSs in term of cybersecurity education maturity.**

- MSs have a series of initiatives (strategy, action plan etc.) in place for cybersecurity in primary and secondary education. However, national approaches vary widely from one country to another and mostly rely on decentralised initiatives or stand at the very early stage of implementation[85].
- While educational initiatives in cybersecurity are generally supported by a national regulatory framework, they rely heavily on national cybersecurity strategies[86].
- Around half of MSs affirm[87] that their country has integrated cybersecurity with national curricula for primary (13 MSs) and secondary education (14 MSs), while several MSs have started discussions on how to integrate cybersecurity with national curricula for primary and secondary education (6 MSs).

## Ongoing work

ENISA has been developing instruments related to role profiles or higher education, notably the European Cybersecurity Skills Framework[88] (ECSF), the Cybersecurity Higher Education Database[89] (CyberHEAD), the Cyber Exercise Platform and the European Cyber Security Challenge[90]. The Cybersecurity Skills Academy is a European policy initiative, part of the 2023 European Year of Skills[91], that aims to close the cyber security talent gap, strengthen the EU cyber workforce and boost EU competitiveness, growth and resilience[92].

## 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.*

**To achieve this recommendation:**

- The national cybersecurity strategy of MSs should include a plan to enhance the general level of cybersecurity awareness among citizens, in accordance with Art.7(1) (h) of the NIS2 Directive. As part of their national cybersecurity strategy, MSs are encouraged to adopt policies promoting and developing educational programmes and training sessions focusing on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities in accordance with Art.7(2) (f) of the NIS2 Directive.
- EU MSs are encouraged to develop programmes with tailored content to address the specific needs of different demographics in order to improve cybersecurity awareness in underserved populations and also to use multiple communication channels such as social media, public service announcements and community events to reach a wider audience.
- Aiming for a common high level of cybersecurity awareness among EU citizens, ENISA could support MSs by organising awareness events and by preparing and promoting relevant material in national languages to facilitate the improvement of cyber hygiene practices among the general population.
- EU MSs are invited to work closely with the European Commission and ENISA towards developing a monitoring framework related to primary and secondary educational programmes addressing the gap in cybersecurity skills.
- EU MSs are encouraged to develop retraining policies and programmes to upskill talent. In this context, they are also encouraged to use the ENISA CyberHEAD database for higher education (European Qualifications Framework, levels 6-7), as the reporting tool to collect relevant EU data, but also to promote its usefulness to citizens looking to upskill their knowledge in the field of cybersecurity.
- EU MSs should encourage providers of services in areas such as telecoms, banking and digital services to invest on cybersecurity awareness as part of their corporate digital responsibility with the possibility of eventually establishing a responsibility framework for corporate cybersecurity applicable to relevant operators.

Chapter III

# INCREASING THE LEVEL OF CYBERSECURITY

A number of particular areas of focus were identified for further analysis with the aim of increasing the level of cybersecurity in the EU. The selection of these areas was based on an analysis that took into consideration the following:

- Indicators of the EU Cybersecurity Index 2024 with the lowest EU average values and/or highest deviation among EU MSs;
- Individual key findings and gaps from other sources, including though not limited to NIS Investments, an assessment the criticality and maturity of NIS1 sectors and an analysis of NCSS;
- Main threats to the Union deriving from the Threat Landscape, Risk Assessment and Foresight findings;
- Specific priorities identified by EU MSs, as expressed in Council Conclusions[93] on the future of cybersecurity, a survey by the NIS Cooperation Group (NIS CG) and ENISA 's discussions with MSs in various fora (e.g. NIS Cooperation Group).

The selected areas were validated by the NIS CG and the European Commission.

## 3.1 POLICY IMPLEMENTATION

### 3.1.1 Implementing a comprehensive and complementary cybersecurity policy framework

As the EU cybersecurity policy framework has evolved over the last few years, implementation at a national level becomes a priority and national competent authorities are already in the process of working towards this goal. However, the **policy implementation process is demanding both in terms of time and resources**. At the time data was being collected, the MSs were introducing the new NIS2 sectors into their national legislation. The expansion in scope and coverage of entities between NIS1 and NIS2 directives is demanding in effort both during the transposition process and for the subsequent supervision of these entities by national competent authorities.

At the same time, **important and substantial EU horizontal legislation (EUCC, CRA, CSOA) has been adopted recently or is about to be adopted.** For instance, in view of the application of the EUCC, MSs are now working on establishing capabilities for assessing conformity including accreditation and notification, market surveillance and enforcement. Similar efforts will need to be undertaken at a much larger scale for the CRA. In addition, **one *lex specialis* to NIS2 (i.e. DORA)** and a few sector-specific implementing or delegated acts **complementary to the horizontal policy framework** (i.e. electricity, aviation) were adopted. The coordination effort needed by the MSs to facilitate coherent implementation on a national level is significant (e.g. on security measures, incident reporting, vulnerability notifications, etc.) and will have to be followed by efforts to ensure compliance by the concerned entities themselves. It is paramount to **avoid fragmentation, duplication or overlap of cybersecurity legislation across the Union with sector specific initiatives or *lex specialis***[94]. The Council has called on the Commission to develop a clear overview of the relevant horizontal and sectoral legislative frameworks and their interplay[95]. Moreover, it is important **to leverage any potential synergies**.

- With respect to the notification of incidents, implementation of the various laws could leverage synergies in order to avoid the creation of multiple, independent data sets on incidents. Fragmentation would limit the benefits to situational awareness of having access to the full picture of information on incidents.
- The impact of various legislative instruments on the entities could also be considered. For instance, data relating to NIS Investments in 2023 reveals that the primary legal driver of cybersecurity investments in the Transport sector is the NIS Directive (55% of the transport OESs who were interviewed report such a driver), followed by transport industry-specific security requirements (27% of the transport OESs) and legal requirements such as GDPR (12% of the transport OESs). The lone exception is the Aviation sector, where sectorial legislative requirements actually top the priorities list over NIS with 45%.
- The issue of skilled resources in order for entities to comply with the new legislative framework has been documented in the 2023 NIS Investments report with over half of the entities within the scope of the NIS planning to hire new cybersecurity staff (median of two new staff members per organisation) over the next two years. Based on discussions with MSs, NCAs will also need to augment their cybersecurity staff in order to address the growing volume of tasks and the expanded scope of NIS2.
- Guidance and support for NCAs is needed to accompany the implementation process, given the wide coverage of the horizontal legislation and also the interplay with other relevant pieces of legislation. Likewise, timely guidance and support provided to entities within the scope can help them better prepare for compliance. Discussions with the MSs highlight the following topics (non-exhaustive):
  - The understanding of the NIS2 scope and annexes;
  - The interpretation of the GDPR in relation to the NIS2;
  - Interpretations of what constitutes a significant incident in various sectors;
  - The way that horizontal and sectorial legislation relates, such as NIS2 and DORA or NCCS, or the way horizontal legislation relates to technology-based legislation such as AI-Act and EUDIF.

## Ongoing work


The NIS CG has established several work streams (e.g. on incident reporting, security measures etc.) to support harmonised implementation of NIS2 across MSs in several dimensions. Moreover, the NIS CG has established interfaces to collaborate with national authorities responsible for the implementation of sectoral legislation to identify and address any potential overlaps and gaps. The input provided by the NIS CG is highly valued and essential for achieving a consistent and harmonised implementation across MSs. This includes the mapping of national solutions and experiences, the discussion of challenges to implementation, and the elaboration of concrete recommendations and guidelines for both the MSs and the EC.

### 3.1.2 Identification and Supervision

When it comes to the national transposition of NIS2, **the process to establish a list of essential and important entities by the MSs is at an advanced stage** (progress is assessed at 62% with 22 MSs close or above this average).

- The majority of the MSs are currently drawing up a list of essential and important entities.
- Around two-thirds of MSs are in the process of creating a list of essential and important entities that are SMEs, while most of the rest have completed this process.
- The list of essential and important entities is expected to be kept up to date (for the majority of the MSs).

**The implementation of supervisory measures varies among MSs**. It appears too early in the transposition process to collect data on compliance to the measures for all entities under NIS2.

- One-third of the MSs indicated that more than 80% of the NIS2 entities are subjected to supervisory measures by the relevant national competent authorities. The rest of the MSs indicate lower percentages that vary.
- Regular cybersecurity audits are performed in more than two-thirds of the MSs, either by a dedicated supervisory authority or by independent third parties. Only a very limited number of MSs has no mechanism to check compliance. The percentage of essential and important entities for which compliance data is collected varies significantly among MSs.

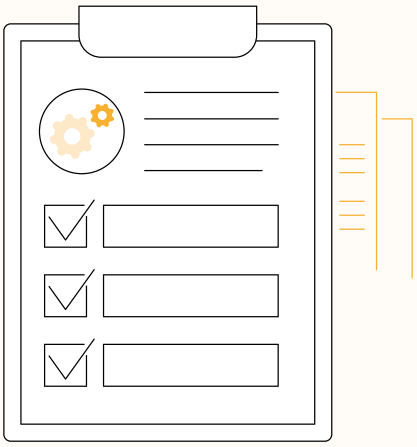
### 3.1.3 Cybersecurity risk management measures

**The majority of MSs have defined cybersecurity risk management measures for essential and important entities.**

- Two-thirds of the MSs have documented cybersecurity baselines for essential and important entities, while the rest are in the process of identifying and documenting them. In addition, 41% of the MSs have established an informal or formal process for reviewing and updating these measures.
- The adoption of legislation setting cybersecurity requirements for the newly added sectors of NIS2 is ongoing in the majority of the MSs.
- Almost all MSs require measures on policies on risk analysis and cybersecurity, incident handling and business continuity. More than two-thirds require the remaining cybersecurity risk management measures defined in Article 21.

It is expected that all the above indicators will change after the transposition of NIS2. Moreover, for the types of entities listed in Article 21(5) a more harmonised EU approach to cyber risk management is foreseen with the adoption, in October, of the Implementing Regulation 2024/2690 on cybersecurity risk management for specific categories of entities providing digital services. We expect that the Implementing Regulation, pursuant to NIS2 Articles 21(5) & 23(11), will reshape and harmonise the cybersecurity risk management measures for the sectors concerned.

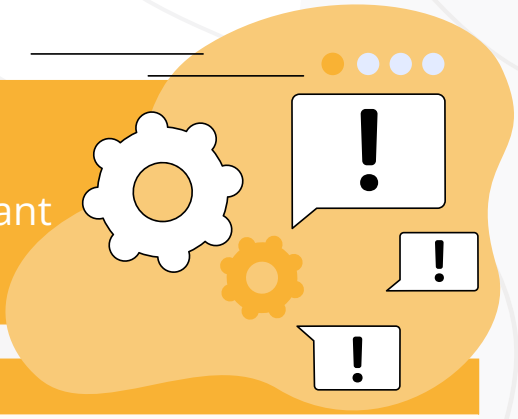
#### Good practices from Member States



Supervision can be carried out differently, depending on the country's needs. Examples include working closely together with the entities on how to assess conformity as well as offering conformity assessment services to the entities on a voluntary basis relying on third-party support.

Info box

# Cybersecurity risk management measures for essential and important entities under NIS2



## Cybersecurity risk management measures (article 21)

Type: **appropriate** and **proportionate technical**, **operational** and **organisational** measures

Aim: (a) to **manage the risks** posed to the security of network and information systems which those entities use for their operations or for the provision of their services and (b) to **prevent or minimise the impact of incidents** on recipients of their services and on other services.

**Risk-based approach**: level of security of network and information systems is **appropriate to the risks posed**, taking into account the **state-of-the art** and the **cost of implementation**.

**Proportionality**: taking account of the degree of the entity's **exposure to risks**, the entity's **size** and the **likelihood incidents may occur** and their **severity**, including their **societal** and **economic impact**.

**All-hazards approach**: protect network and information systems and the **physical environment** of those systems from incidents.

- **Policies** on risk analysis and information system security;
- **Incident handling**;
- **Business continuity**, such as **backup management** and **disaster recovery**, and **crisis management**;
- **Supply chain security**, including security-related aspects concerning 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 **cyber 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**;
- The use of **multi-factor authentication or continuous authentication solutions**, **secured voice, video and text communications** and **secured emergency communication systems** within the entity, where appropriate.

When it comes to the implementation of cybersecurity risk management measures, we see **significant deviations among entities, which are dependent on the size of the company and the maturity of the sector.**

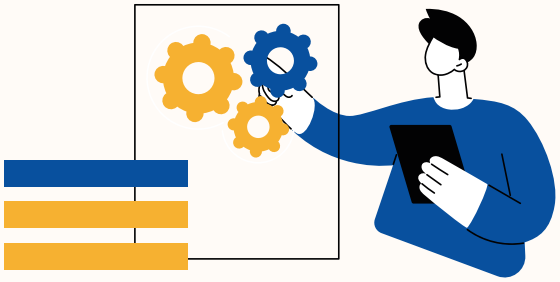
- In 2023, Operators of Essential Services (OESs) and Digital Service Providers (DSPs) under the NIS1 Directive[95] spent 11.9% of their IT FTEs on information security, a decrease of 0.1% compared to 2022, despite the overall increase in cybersecurity spending[96]. At the same time, the percentage of IT budgets going to cybersecurity varies significantly among sectors, ranging between 5% and 10%.
- 45% of the OESs and DSPs declared good or mature cyber risk management capabilities, while 23% declared having only limited or none such capabilities[97]. Likewise, 49% declared good or mature incident detection and response capabilities, and 18% limited or none such capabilities. In both of these areas, we noted wide deviations between sectors, with higher maturity being assessed in sectors such as Banking, Energy, Healthcare and Transport, and lower maturity in sectors such as Digital infrastructures and Drinking water.

- According to Eurostat, as of 2022:
  - 83% of large enterprises in the EU apply at least one ICT security measure[98] with 25 member states close to or above this figure. The percentage drops to 49% when considering SMEs in the EU. The portion of companies that apply all these ICT security measures is 17% for large enterprises and 4% for SMEs. Moreover, the measures examined by Eurostat are only a fraction of the measures under NIS2 for essential and important entities.
  - 80% of large enterprises have documented measures, practices or procedures on ICT security and 58% have defined or reviewed an ICT security policy within the previous 12 months (data collected in 2022). But for SMEs, the numbers are much lower; 36% have documented measures, practices or procedures on ICT security and 23% have defined or reviewed an ICT security policy within the previous 12 months.
  - 72% of large enterprises perform risk assessments to assess the risk of ICT security incidents, compared to 31% of SMEs.

Overall, **the involvement of top management in cybersecurity affects significantly whether security measures are implemented**. The maturity of risk management, incident detection and response, and the management of cyber risk by a third party are strongly correlated with the involvement of top management.

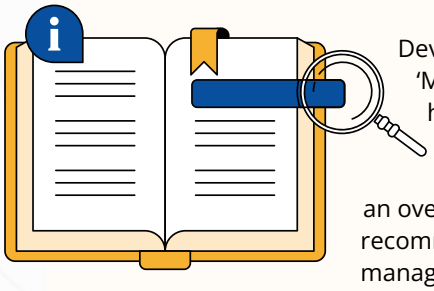
- Leadership approves management measures for cybersecurity risk in 81% of the OESs and DSPs we surveyed in 2023[99]. For 50% of these organisations, leadership attends dedicated cybersecurity training.
- We also observed a very strong correlation between the involvement of top management in cybersecurity and an organisation's maturity in the management of cyber risk and in its incident detection and response capabilities. In both cases, organisations whose leadership is active in cybersecurity are more than twice as likely to score above the basic level.

## Ongoing work



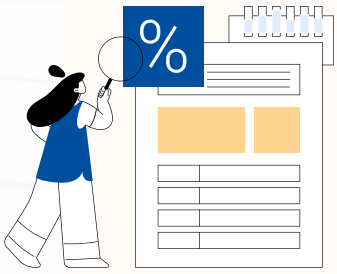
In the past, the NIS CG and ENISA had created a guideline on cybersecurity measures aimed at the entities to assist with conformity. The cybersecurity measures were mapped to international standards and good practices. ENISA is currently preparing a similar document in collaboration with European Commission and the NIS CG. On a national level, MSs are also developing guidance for NIS entities on how the NIS2 measures for cybersecurity risk management match national or international standards.

## Good practices from Member States



Development of a 'Managing Cyber Risks' handbook aimed at senior management, providing an overview and recommendations for managing cyber risks. It formulates six basic principles to help management and supervisory boards analyse cyber risks and is complemented by a toolkit of helpful questions and answers to raise awareness of cyber security at senior management level.

## Good practices from Member States



Monitoring the implementation of cyber risk management measures in a particular sector (e.g. public administration) can be achieved by collecting national statistical information via a self-assessment tool or audits.

### 3.1.4 Information sharing and reporting obligations: institutional framework and practice

A functioning cooperation among relevant actors is a pre-requisite for the effective sharing of information. The NIS2 Directive outlines obligations for national-level cooperation, applying to competent authorities, single point of contacts (SPOCs), and CSIRTs[100] (hereby referred to as 'NIS2 entities'). They are expected to cooperate among themselves and also, to various degrees, with the authorities responsible for specific domains, e.g. those competent for the financial sector under DORA[101]. **Overall, the state of national cooperation is fairly good; the MSs that have not yet reached full maturity in terms of cooperation among NIS2 entities are taking action to progress. However, cooperation between NIS2 authorities and competent authorities under other pieces of EU legislation is lagging behind in some MSs[102].**

- Based on ENISA data[103], all MSs have either established or are defining mechanisms for cooperation among NIS2 entities. This also includes the notification of incidents, threats and near misses to CSIRTs or competent authorities[104]. More than two-thirds (21 MSs) have either implemented or are in the process of implementing the flow of such information from the CSIRTs or competent authorities to the national single point of contact[105].
- All MSs have either implemented or are defining measures to ensure that the NIS2 competent authorities and the authorities competent for critical entities (under the Directive 2022/2557)[106] cooperate and exchange information on a regular basis, e.g. on risks, threats and incidents affecting critical entities[107].
- About two-thirds of MSs have taken action to ensure that the NIS2 competent authorities exchange, on a regular basis, information on cyber incidents and threats with the authorities competent for electronic identification and trust services (Regulation 910/2014 - eIDAS) (19 MSs); for the financial sector (Regulation 2022/2554 - DORA) (17 MSs); or for electronic communications services (Directive 2018/1972 - EECC) (18 MSs).

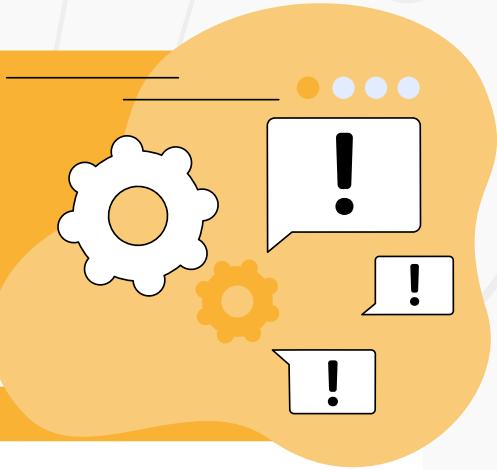
One of the most prominent areas of information sharing concerns cybersecurity incidents. A number of EU legal acts contain provisions (and, in some cases, obligations) for entities falling under their respective remit to report incidents to the competent authority. The implementation of reporting provisions relies on the establishment of dedicated processes and tools, as well of a common understanding of what constitutes an incident and how it shall be communicated. NIS2[108] (formerly NIS1), European Digital Identity Framework (EUDIF formerly eIDAS[109]) and EECC[110] are the main pieces of EU legislation mandating the reporting of incidents with a significant impact[111]. They apply respectively to essential and important entities, trust services providers and telecommunication services providers[112].

**The implementation of obligations to notify incidents and the application of contextual measures are generally advanced, although the implementation of the requirements of NIS2 is still ongoing and some MSs lack dedicated reporting tools. The coherent implementation of reporting obligations across EU legislation and MSs will be crucial for the effectiveness of such requirements.**

- Based on data ENISA collected from the MSs, the introduction of legal provisions for the notification of incidents, to ensure that specific organisations notify the relevant authorities of incidents with a significant impact, is almost complete for providers of telecommunication services providers (as per Article 40 of the EECC) (24 MSs) and trust services providers (as per Article 19 of the eIDAS Regulation[113]) (25 MSs). The implementation of notification requirements for essential and important entities mandated by NIS2 Article 23 is still progressing (15 MSs). It is to be noted that NIS2 Article 23.11 gives the EC the possibility of adopting implementing acts to further specify the type of information, the format and procedure for the notification of an incident. The article also requires the EC to adopt implementing acts further specifying, for certain types of entities, the cases in which an incident is considered to be significant. This is currently being done for the digital infrastructure and ICT service management sectors, a practice that could be extended to other sectors where streamlined and harmonised guidance at the EU level would be beneficial.
- Most MSs (23 MSs) have defined and documented a national taxonomy for the classification of cyber-incidents, as well as thresholds for their evaluation (24 MSs). Dedicated tools to facilitate the reporting processes have been put in place in 22 MSs.
- The review of NIS1 was driven, among other factors, by the fact that MSs interpreted incident reporting requirements differently. This issue might persist as MSs might operationalise the reporting requirements of EU legislation (e.g. NIS2, DORA, NCCS[114] and Aviation[115]) in differing ways, with national contexts and specificities sometimes making it difficult to align on notification timelines and the definition of incidents.

Info box

# Main incident reporting obligations in the EU legislation



## NIS1 compared to NIS2

### NIS 1

**Article 13** sets the obligation for Member States to ensure that **operators of essential services (OESs)** notify the competent authority or the CSIRT of **incidents having a significant impact** on the continuity of their services.

**Article 16** sets the obligation for Member States to ensure that **providers of certain digital services** (online market places, online search engine, cloud computing) (so called Digital Service Providers - '**DSPs**') notify the competent authority or the CSIRT of any **incident having a substantial impact** on the provision of their services.

### NIS2

**Article 23** sets the obligation for Member States to ensure that **essential and important entities** notify any **incident that has a significant impact** on the provision of their services.

**Note**: The deadline for the Member States to transpose the Directive was 17 October 2024.

## eIDAS Regulation compared to the European Digital Identity Framework

### eIDAS Regulation

**Article 19** sets the obligation for qualified and non-qualified trust service providers to notify **any breach of security or loss of integrity that has a significant impact** on the trust service provided or on the personal data maintained therein.

### European Digital Identity Framework (EUDIF)

The reporting obligations for trust service providers falling under the scope of NIS2 will be driven by NIS2 provisions, as explained in recital 50. Some reporting obligations are still set by EUDIF. In particular articles 19a and 24.2 require, respectively, non-qualified and qualified trust service providers to notify any security breaches and service disruptions with a significant impact on the service or the personal data maintained therein. **Note**: The European Digital Identity Framework entered into force in May 2024.

## EECC

**Article 40** sets the obligation for Member States to ensure that providers of public electronic communications networks or of publicly available electronic communications services notify **security incidents that have a significant impact** on the operation of networks or services. It is to be noted that EECC Art. 40-41 is repealed by NIS2 as of 18 October.

## DORA

**Article 19** mandates the reporting of major ICT-related incidents to the relevant competent authorities.

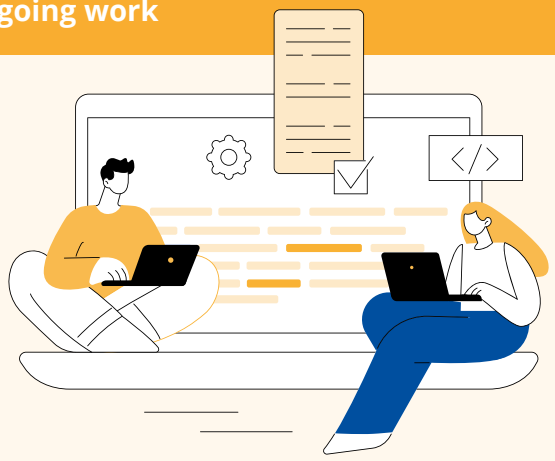
## Aviation

Organisations shall report any event having an actual adverse effect on the security of network and information systems[116].

**The number of incidents reported shows consistency over the years (EECC) or an increase (NIS1, eIDAS). This can be explained by the threat landscape, but it is likely also a sign of progress both in the maturity of the reporting frameworks themselves as well as in the reporting capabilities of the entities concerned. Still, the number of reported incidents seems to be low, which probably means that incidents are under-reported.**

- In terms of actual reporting, the reporting framework of the EECC seems to be the most established, with a steady annual number of reported incidents over the last ten years.
- The number of significant incidents affecting OESs and DSPs under NIS1 increased from 880 incidents reported in 2022 to 1049 in 2023[117]. Similarly, the number of reported security breaches affecting trust services (eIDAS) also increased significantly in 2023 with respect to the past[118].
- Although the data above concerns only incidents with an impact considered 'significant', hence a sub-set of the overall number of incidents, their number has been assessed as probably underestimated based on discussions with the NIS CG and the general reluctance of organisations to share this kind of information (see first bullet point). Still, it is difficult to determine with precision whether all incidents with a significant impact have been reported:
- The ENISA NIS Investment studies indicate that, in 2021 and 2022 respectively, 11% and 6% of the surveyed OESs and DSPs declared that they had experienced a major security incident. However, 12% and 10% respectively did not want to disclose this kind of information.
- According to Eurostat[119], in 2022 there were 30,017 large enterprises working in relevant sectors in the EU[120]. Assuming that all of them were OESs or DSPs and that each incident was reported by a different OES or DSP and taking into account the year when most significant incidents were reported (2023, with 1,049 incidents for both OESs and DSPs), this suggests that approximately 3.5% of OESs/DSPs in the EU have experienced a significant incident.
- In 2019, the total number of OESs that were reported to the Commission by Member States ranged from 20 to 10,897 with an average of 633 OESs per Member State[121]. Again, taking into account the significant incidents reported in 2023, and assuming that each incident was reported by a different OES, approximately 6% of OESs in the EU have experienced a significant incident.

## Ongoing work



In 2022 ENISA began developing capabilities to be able to monitor, collect and analyse incident vulnerabilities using information shared with the Agency on a voluntary basis by stakeholders (including MSs and Union entities) or due to legal requirements. In particular, the Agency has developed structured cooperation with CERT-EU and intensified cooperation with other relevant Union entities such as the EEAS, Europol EC3 and the Commission. This allowed the Agency to build situational pictures both on a regular basis as a preparedness tool as well as to provide input during large-scale incidents or crises. A key example of this work is the Quarterly EU Joint Cyber Assessment Report developed by the Agency together with CERT-EU and EC3 and with contributions from MSs that provide a regular situational picture about incidents, vulnerabilities and threats impacting the EU. This report maps the requirements outlined in CSA Art. 7(6) as well as being described in the Blueprint. The Agency is working on further integrating input from various communities including private sector and international partners[128].

The European Commission is developing, in collaboration with ENISA and CERT-EU, a cybersecurity Situation Centre to collect and integrate information from relevant sources and provide a real-time overview of the threat landscape to the EU bodies.

# 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.*

**To achieve this recommendation the following actions are suggested.**

- ENISA and/or the EC should consider mapping the various legal requirements deriving from EU horizontal and sectoral cybersecurity policies. In this context, the NIS Cooperation Group, EU-Cyclone and the EU CSIRTs Network could be used to increase joint understanding of the complex elements of cybersecurity legislation such as the NIS2 Directive, amongst others such as the scope, incident reporting thresholds and security measures.
- The EC with the technical support by ENISA, should help MSs ensure a unified approach on baseline cybersecurity risk management measures for essential and important entities. NIS2 article 21.5 mandates the EC to adopt implementing acts laying down the technical and methodological requirements for certain entities for certain sectors within the scope of NIS2 and provides the possibility to do so for other such sectors. It is important that applicable measures are discussed with all the stakeholders concerned, and in particular with the sectors involved, to ensure a smooth implementation and take-up.
- ENISA should support the MSs with non-binding guidance on risk management aimed at entities and for specific sectors, taking into account standards and good practises. Such guidance could address implementation challenges faced by specific sectors in the NIS2 Directive or by SMEs and start-ups.
- The NIS Cooperation Group, with the support of ENISA and the EC, should establish a single common EU framework (including templates and data fields) to report incidents under NIS2. Such a framework could be the basis for exploring alignment with other reporting frameworks under other EU legislation. The framework could take into account the different maturity levels of reporting practices and aim to reduce the administrative burden on the entities and on the authorities. The framework could also allow for post-incident analysis, which can offer valuable insights to the entities concerned and act as an incentive for reporting.
- To support entities in their compliance with upcoming regulatory requirements, the MSs (e.g. via the NIS CG), with the support of ENISA, could establish information sharing platforms with private sector entities to discuss implementation challenges and foster collaboration and alignment.
- To address challenges in terms of resources, external support could be made available to national competent authorities that deal with the supervision of the NIS2 Directive (e.g. via an EU support action).

## 3.2 CYBER CRISIS MANAGEMENT

Cybersecurity crisis management at EU level has matured significantly in past years. At the time of the adoption of NIS1, in 2016, EU-level cooperation on crisis management was still a relatively new area. The Commission's recommendation on coordinated response to large-scale cybersecurity incidents (so called 'Blueprint')[122], adopted in 2017, addressed the roles of all relevant actors[123] and identified the need for a mechanism at operational level to connect technical and political levels. Accordingly, the EU-CyCLONe network of national cyber crisis management authorities was set up on an informal basis in 2020. Since then, the situation has evolved rapidly; in 2022 NIS2 was adopted, including provisions covering cyber crisis management at the levels of the EU and MSs, and involving specific organisations such as important and essential entities. In particular, NIS2:

- Formalises the establishment of a European cyber crisis liaison organisation network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises at operational level[124], and strengthens the role of the CSIRTs Network[125], composed of CSIRTs appointed by EU MSs and tasked, among other things, to promote swift and effective operational cooperation among them;
- Mandates the designation of national authorities responsible for the management of large-scale cybersecurity incidents and crises and the adoption of national large-scale cybersecurity incident and crisis response plans[126];
- Mandates MSs to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures, including on crisis management.

To complement the framework of NIS2, it is important to mention the CSOA, which further strengthens the context for cybersecurity crisis management; for example, it foresees a European Cybersecurity Alert System, made up of Cyber Hubs interconnected across the EU, and a comprehensive Cybersecurity Emergency Mechanism.

Also relevant is the Cyber Crisis Management Roadmap developed in the Council under the Czech Presidency in 2022.

**This evolution of crisis management has brought into the picture new actors, roles and tasks. In this context, the Council in May 2024 called on the Commission to swiftly evaluate the current Blueprint and, on this basis, propose a revised one in the form of a Council recommendation.**

The Council Conclusions also emphasise the need for compatibility of cyber crisis management with existing and emerging EU crisis management frameworks, procedures and structures.

In parallel, the legislative framework needs to be matched with joint technical capabilities and mutual assistance. For example, work is also being done to support the technical capabilities of MSs to prevent and respond to large-scale cyberattacks. Notably, ENISA provides both ex-post services for incident management and response, as well as ex-ante services such as the assessment of capabilities[127].

This section focuses on three important aspects of European crisis management: situational awareness, the capabilities of MSs and, in particular, of their CSIRTs and CSIRTs Network's members and MSs participation in cyber exercises, intended as an indicator of preparedness.

### 3.2.1 Situational awareness

The foundation of crisis management is the availability of information and the capability to process it. Cyber threat intelligence (CTI), open-source intelligence (OSINT), data from private sources and from governmental sources, reporting of incidents and near misses; these are only some examples of the information sources that allow the monitoring and analysis of cyber threats, events and incidents that ultimately will lead to the cyber situational awareness needed for crisis management.

**In order to support reliable and solid situational awareness at the EU level, several initiatives are being carried out by European Union institutions, bodies and agencies, such as the European Commission, ENISA, the EU Intelligence and Situation Centre (EU INTCEN), CERT-EU and Europol's European Cybercrime Centre (EC3). Still, a common, real-time picture encompassing all MSs and covering all aspects of situational awareness is missing.**

MSs also monitor their national cyber space and strive to share relevant information in a timely manner across the country and, when relevant, at the EU level[129]. **Overall, all countries monitor their cybersecurity threat level; however there are significant differences on the monitoring frequency and alerting modes. The latter is not necessarily an issue, while the former signals a lack of capabilities in some MSs[130].**

- All countries are endowed with the means for monitoring the cybersecurity threat level nationally, which almost two-thirds of Member States (19 MSs) use daily or 24/7. The remaining MSs monitor the threat level weekly, monthly or only on specific occasions.
- In case of need, all MSs are equipped to communicate the threat level to essential and important entities, either in a manual/ad-hoc manner (13 MSs) or with minimum human intervention (14 MSs). While timeliness of information sharing is obviously crucial in the context of a crisis, the choice of the means of communication (manual vs automated) does not necessarily reflect the level of maturity, as it can be dictated by factors such as a more limited number of essential and important entities or a more tailored approach to alerting.

Single organisations perform threat monitoring also; for example, a company might have its own Security Operation Centre (SOC) to detect and respond to cyber threats and/or it could access relevant information by purchasing Cyber Threat Intelligence from specialised companies. Another way for organisations to access and also to exchange information is through participation in industry associations or Information Sharing and Analysis Centres (ISACs), i.e. organisations that provide a central resource for gathering information on cyber threats, root causes and incidents as well as sharing experience, knowledge and analysis[131]. Comprehensive public data on the actual monitoring capacity of enterprises is scarce, however **ENISA data shows that the capabilities of OESs/DSPs to collect and exchange information are not yet mature. A large share of OESs/DSPs does not have a Security Operation Centre (SOC) and – with some exceptions – they do not invest significantly in CTI. This share is much bigger for SMEs. ISACs have emerged as a successful tool to share information at the EU level.**

- According to the ENISA NIS Investments Report 2022[132], 37% of the OESs and DSPs do not operate a dedicated Security Operation Centre (SOC) and this figure increases to 76% for SMEs.
- OESs and DSPs spend on median EUR 50,000 per annum on Cyber Threat Intelligence (CTI), though data indicates that most organisations do not earmark vast budgets for CTI, while larger operators — especially within the banking sector — do invest significantly in CTI. Considering that CTI is a valuable source of information in the context of incident prevention and risk assessment, this finding seems to indicate a need to provide easier access to CTI, especially for smaller OESs and DSPs.
- The ENISA NIS Investments Report 2023[133] shows that 70% of OESs and DSPs engage in collaboration or information-sharing initiatives and most of them do so by using ISACs, either at the EU level (36% of the total) or national level (9%). ISACs have emerged as a successful tool to share information – especially at the EU level – as sectors featuring European ISACs have the highest rates of participation in any kind of information sharing activities. Still, such information sharing activities often limit access to SMEs, since 56% of SMEs do not engage in similar activities.

It is to be noted that monitoring capabilities at the organisational level do not necessarily translate to better situational awareness at the national or EU level. As highlighted in section 3.1.4, despite important advances, **the significant cybersecurity incidents reported at the EU level are probably only a sub-set of the incidents that actually took place and, in general, enterprises, especially SMEs, might not report e.g. for reputational reasons, lack of awareness or obligation to report. Indeed, the share of SMEs that declared that they have not experienced incidents is strikingly high, when compared to large enterprises.**

- According to Eurostat, which regularly conducts a survey among enterprises on their ICT security[134], the number of enterprises in the EU declaring that they have experienced at least one ICT security incident in 2021 is 22.2%[135], although the source of the incidents is generally non-malicious[136]. It needs to be pointed out that entities are generally reluctant to report incidents[137] e.g. to avoid damage to their reputations.
- The biggest share of the incidents declared led to the unavailability of ICT services, though the experiences of large enterprises and SMEs differed significantly in this respect; 65.9% of large enterprises and 82.3% of SMEs did not experience such incidents. Although large enterprises likely experience more incidents[138], the relatively high share of SMEs that have not experienced security incidents is somehow striking and might indicate an even more marked reluctance in 'admitting' they had suffered from such an incident.
- Further analysis does not indicate substantial differences for incidents leading to data destruction/corruption or disclosure of confidential data; on average, more than 90% of both large enterprises and SMEs did not experience such security incidents in 2021.

### 3.2.2 National CSIRTs

CSIRTs have important operational functions in the collaboration and co-ordination both at the national level and between national and international communities and organisations[139]. CSIRTs act as a first line of response to cyber incidents and often act as producers of situational awareness for the public, businesses and decision-makers. As such, CSIRTs and those that are part of the CSIRTs Network in particular form a crucial part of EU cyber infrastructure and can be considered the technical frontline for incident response. Therefore, their relationship with cyber crisis management authorities and EU-CyCLONe is crucial.

**Members of the CSIRTs Network are well-integrated in the wider international networks dealing with security issues. Their maturity, in terms of compliance with internationally recognised practices, could improve. This aspect is more pronounced among CSIRTs that are not part of the Network. Scalability of CSIRTs' tooling, also in support of processes automation, could help both in harmonising maturity and capabilities across the EU.**

- The ENISA CSIRTs Inventory[140] lists 675 CSIRTs in the MSs, of which 39 are members of the CSIRTs Network.
- Most of the CSIRTs Network members (77%) are also members of FIRST, the Forum for Incident Response and Security Teams, which is an indicator of their integration in wider networks to deal with security issues. About one-third of them (31%) are either certified or candidates for (re)certification under Trusted Introducer (TI) meaning that their security incident management procedures, infrastructures and response capacity are aligned with internationally recognised standards.
- These percentages are significantly lower among the CSIRTs that are not part of the network; about half (46%) are members of FIRST and only 7% are either certified or candidates for (re)certification under Trusted Introducer.
- In the last few years, CSIRTs witnessed a sharp increase in the constituency they serve; for example, more sectors are considered as important or essential in NIS2 and the CSIRTs' role in the case of cybersecurity crises has been strengthened. CSIRTs also have a role in vulnerability management under CRA. In light of this, the efficacy and efficiency of procedures will probably need to rely on tools that support the automatization of processes and that are scalable and interoperable across the EU.

### 3.2.3 National capabilities: Cyber-exercises

The management of a cyber crisis starts before the crisis itself begins, with specific actions to ensure preparedness. The organisation of simulation exercises to test procedures, cooperation and fluidity of action in the event of a crisis is regarded as an important component of crisis management. In general, the objectives of exercises are to test processes at the EU and national levels, improve network coordination and detect or resolve vulnerabilities, raise awareness of players' capabilities and train leadership and staff[141]. In 2023, the exercise Blue Olex gathered together the high level executives of competent authorities in 27 MSs who are in charge of cyber crisis management and/or cyber policy, the EC and ENISA. It was an opportunity for these actors to exercise their interactions with the newly formed EU-CyCLONe network at the EU level[142]. Shortly afterwards, representatives from national electoral and cybersecurity authorities came together for the exercise 'EU ELEx'[143] to evaluate and strengthen their working methods should potential cybersecurity incidents affecting the European elections occur. Lastly, this year in June, the 7th edition of the exercise 'Cyber Europe 2024' took place. Cyber Europe is a series of pan-European exercises organised bi-annually by ENISA, together with the MSs and other European bodies. The exercise's scenario envisioned attacks on the energy sector across the EU, that would also be targeting digital infrastructure and public administration as secondary objectives to increase pressure and incite chaos[144].

**Participation in EU-level exercises is high, but it is not always matched by structured national exercises, which might weaken the EU's overall capacity to deal with a cybersecurity crisis. It has been noted that exercises are being organised under several frameworks, hence avoiding 'exercise-fatigue' will be an ever-important factor to ensure the effectiveness of this high level of participation in exercises.**

- Based on ENISA data[145], most MSs (24) conduct cyber exercises, either at the national or EU/international level and involve both the private and the public sectors (22 MSs). Indeed, participation in cybersecurity exercises organised at the EU-level is high.
- About half of MSs (12) has a defined and established programme at the national level but fewer (11) feature a process to incorporate lessons learnt and new testing needs. Although some MSs use international exercises to also test national procedures, the lack of structured national exercises might weaken the national foundations of EU-level crisis management.

*A common, real-time picture encompassing all Member States and covering all aspects of situational awareness is missing.*

**In order to support EU-level situational awareness, several initiatives are being carried out by EU institutions, bodies and agencies.**

# 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.*

Without prejudging the role of the mandated actors, crisis management could be enhanced as follows.

**Share situational awareness**

- MSs and national CSIRTs could seek to improve common situational awareness at the national and cross-border levels through their participation in the CSOA European Cybersecurity Alert System and leverage their opportunities for the development of interoperable tools, infrastructures and services.
- As per the CSA, Article 7(6), ENISA, in close cooperation with the MSs, prepares regular in-depth EU Cybersecurity Technical Situation Reports on incidents and cyber threats (JCARs). ENISA and the MSs could improve collaboration on situational awareness to ensure coverage of the whole EU; MSs could increase their active participation in structure and tools (e.g. CSIRT Network) to exchange information, while consolidation of data and analysis could happen at the EU level by strengthening existing mechanisms concerning information flows between both the MSs and the EU, as well as among EU bodies.

**Enable effective and timely response and clear communication**

- EU MSs and Union entities could further streamline and consolidate crisis management processes in order to be able to constitute a stronger common front for incident management and response. This can be achieved by increasing synergies and coherence among crisis management mechanisms, procedures, tasks and actors, as well by defining with more precision the mandate and responsibilities of each actor.
- EU MSs could consider measures in their national cybersecurity programmes to facilitate participation in information sharing initiatives and access to CTI for the entities under NIS2.
- EU MSs could prioritise the maturity of CSIRTs (e.g. by supporting their certification) as well as ensuring adequate tooling e.g. through coordination within the CSIRTs Network on the development – also at the EU level – of tools that support the automatization of processes, and that are scalable and interoperable across different countries.
- EU-CyCLONe could define a strategy to ensure that participation in exercises is optimised to ensure coherent coverage of relevant aspects, including a stock-taking of national capabilities (e.g. by sharing information on different exercises being organised to facilitate rationalisation) and taking into account the latest risk scenarios at the EU level such as those developed under the cyber posture process (https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors).

## 3.3 CYBERSECURITY SKILLS

In an evolving cybersecurity landscape with geopolitical uncertainties, cultivating a cybersecurity culture through awareness, retaining cybersecurity talent and improving relevant skills are crucial aspects for addressing current and upcoming challenges. Putting people at the centre of the digital transformation of our societies and economies is at the core of the EU's vision for the Digital Decade[146].

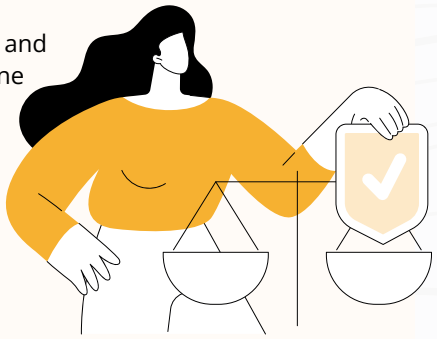
**Cybersecurity skills: While the demand for people with ICT and cybersecurity skills is rapidly increasing, the cybersecurity skills and talent shortage is growing too.**

- Companies are facing severe difficulties in finding appropriate candidates, when they have open positions[147]. The lack of available cybersecurity professionals is a major concern, as around 70% of the companies surveyed that tried to hire staff with skills in cybersecurity (over the last 12 months) experienced difficulties in recruitment.
- According to the same analysis[148], 76% of employees in cybersecurity-related roles did not receive any formal qualification or certified training. Almost one-third entered the role from a non-cyber related role, while more than half of employees absorbed cybersecurity responsibilities into an existing role.
- Regarding the demand for skills, almost half of OESs and DSPs (under NIS1) plan to hire information security FTEs in the next two years aiming to hire an average of 4 FTEs[149]. Most of these hires are expected in the domain of cybersecurity operations (56%), followed by IT security architecture and engineering (42%) and cybersecurity governance and risk (36%).
- 83% of OESs and DSPs claim they experience recruitment difficulties in at least one information security domain, especially in the domain of IT security architecture and engineering (34%)[150].
- The talent shortage affects all types of companies, including SMEs, which represent 99% of all businesses in the EU[151]. In fact, things may be worse for SMEs as it was admitted that 'there is a shortage of skills regarding cybersecurity'; in fact, they claim to be facing difficulties in hiring for any cybersecurity domain[152]. On top of that, it was admitted that SMEs usually do not have a Chief Information Security Officer (CISO), but rather assign the relevant role to someone within the organisation, who may not have the necessary cybersecurity skills and competencies.
- The ENISA Foresight Cybersecurity Threats 2030[153] exercise has revealed that the skills shortage remains among the list of top 10 threats, while its long-term perspectives have intensified somewhat, climbing from number 8 to number 2 of the relevant future challenges from 2023 to 2024.
- Finally, based on a recent Eurobarometer analysis[154], only 18% of companies seem to be aware of the European Cyber Security Skills Framework.

**Diversity and Inclusion: Gender imbalance in cybersecurity roles in the EU**

- When it comes to diversity and inclusion, according to a recent Eurobarometer analysis of cyber skills[155], 70% of companies surveyed agree that diversity and inclusion in cybersecurity are important in their organisations.
- However, while two-thirds of companies agree that women are encouraged to take up roles and tasks in cybersecurity, 56% of companies do not have any women in cybersecurity roles[156].
- The ENISA 2023 NIS Investments data disclose[157] that OESs and DSPs employ an average of 11% of women in information security FTEs, while the median is zero percent, meaning that most of the organisations surveyed do not employ any women as part of their information security FTEs.
- The ICT sector suffers from a severe gender imbalance in the EU with 81% of employed ICT specialists in 2022 being male while women account for 51% of the European population[158].

### Ongoing work



Embracing diversity and gender balance is one of the aims of the EU Cybersecurity Skills Academy (see below for more information on the Academy). With a special focus on upskilling and reskilling women, the goal is to have gender convergence in cybersecurity positions by 2030. Several EU-level initiatives have been established in this regard, such as the EU Gender Equality Strategy[159], Women4Cyber[160], Women in Digital Scoreboard[161] and Concordia Women in Cyber[162].

## Good practices from Member States

Proactive engagement with private sector organisations through regular meetings, fostering awareness and explaining the NIS2 Directive's requirements and their relevance to their businesses.

Dedicated resources to support SMEs in improving their cybersecurity awareness and practices, such as a centralised hub with explanations of common cyber threats, step-by-step guides and downloadable resources or leveraging Public-Private Partnerships (PPPs) for SMEs so as to support enterprises with no internal capacity and expertise.

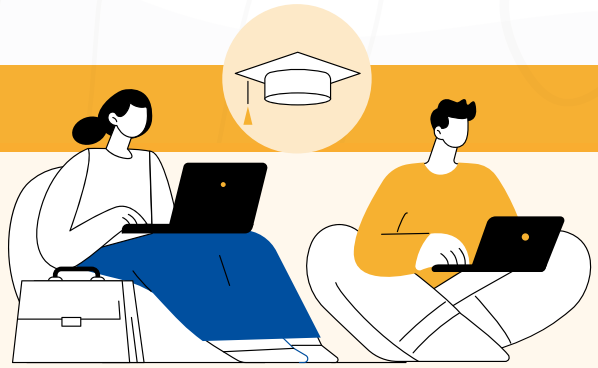
**Cybersecurity training and awareness in enterprises: Enterprises in Europe understand the importance of cybersecurity but taking relevant action remains a challenge. SMEs lag in cybersecurity awareness compared to large enterprises.**

- There is a general consensus among companies with one or more employees that cybersecurity is a matter of high priority (71%)[163].
- Still, the numbers show that almost three-quarters (74%) of companies have not provided any training or awareness raising about cybersecurity for their employees during the last twelve months (from April 2023 until April 2024)[164].
- In most cases (68% of companies) there is a strong consideration and perception that no training or awareness raising about cybersecurity is needed[165].
- In the case of Small and Medium Enterprises (SMEs), about half of the companies (54%) make their employees aware of ICT-related obligations[166], while this is the case for almost all large enterprises (99%) This observation suggests that SMEs do not prioritise cybersecurity awareness training due to immaturity, lack of recognition of its importance or budget constraints.
- These findings are aligned with the observations made in a recent ENISA report, which states that the low level of cybersecurity awareness of personnel is considered one of the seven major challenges identified for SMEs[167].

**Enterprises' Cyber hygiene: The state of cyber hygiene[168] in the EU reveals a concerning gap between SMEs and large enterprises.**

- Almost all large enterprises in the EU[169] are using at least one of the following ICT security measures, strong password authentication, a combination of at least two authentication mechanisms, encryption techniques for data, data backup to a separate location, network access control, VPN, maintenance of log files for analysis after security incidents and performance of ICT security tests.
- Almost one-fifth of SMEs have defined or most recently (within the last 12 months) reviewed their ICT security policy, a finding that has not improved since 2015[170]. This may indicate a lack of cybersecurity awareness, management commitment or skilled personnel. In contrast, the respective percentage for large organisations is 58%, an improvement of almost 15 percentage points since 2015.
- While almost 80% of large enterprises have document(s) on measures, practices or procedures on ICT security, only one-third of SMEs maintain such documentation[171], which could be due to limited resources among other reasons.

## Ongoing work



ENISA is mandated to support closer coordination and the exchange of best practices among MSs on cybersecurity awareness and education, as shown in the Cybersecurity Education Roadmap and demonstrated through initiatives such as the European Cyber Security Challenge, the European Cybersecurity Skills Framework and the Cybersecurity Higher Education Database, known as CYBERHEAD.

The European Commission has recognised and responded to the skills shortage, by adopting and launching the Cybersecurity Skills Academy[172], which is aimed at fostering knowledge generation through education and training by working on a common framework of profiles for cybersecurity roles and associated skills, ensuring a better channelling and visibility over available funding opportunities for skills-related activities, calling on stakeholders to take action and defining indicators to monitor the evolution of the market.

# 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.*

**To achieve this recommendation:**

- ENISA and the European Commission are encouraged to conduct an advanced skills gap analysis using the European Cybersecurity Skills Framework to identify discrepancies between the supply of cybersecurity skills and industry's needs and demand as identified. MSs are invited to work closely with the EC and ENISA towards developing a monitoring framework related to workforce supply and demand.
- To address the workforce shortage, EU MSs could ensure that a cybersecurity workforce strategy is reflected in their national cybersecurity strategies and incorporate elements related to awareness, skills and education in accordance with Arts. 7(1) (h) and 7(2) (f) of the NIS2 Directive and that, in particular, the lack of cybersecurity professionals is addressed. MSs could propose in their roadmaps concrete actions on attracting and retaining cybersecurity specialists. MSs could include measures and funding in their national cybersecurity strategies, targeting SMEs in particular, to boost cyber hygiene and cybersecurity investments in SMEs. Mentorship programs launched by MSs could be a powerful tool to address the gender imbalance. Efforts could also encourage the reskilling of employees, who come from other disciplines.
- Considering the significant number of cyber incidents targeting public administration, MSs are advised to provide training for public sector employees on cybersecurity awareness and hygiene.
- Initiatives at European and national level conducted by public and private entities (PPP) to address shortages in the cybersecurity labour market should be structured and systematic.
- ENISA and/or the EC are advised to expand training programmes, increasing accessibility across industries, and fostering public-private partnerships.
- When it comes to certification of cybersecurity skills in professionals, ENISA should initiate the development of mutual agreements and the creation of a European Cybersecurity Skills Framework profile for specific attestation schemes.
- The EC is invited to consider mobilising EU funds for EU funded masters and PhD degrees under current or newly targeted issues due to the urgency of the EU's security needs. Specific examples could involve the mobilisation of Erasmus Mundus thematic masters and Marie Sklodowska-Curie Actions.
- The European Parliament is encouraged to consider establishing special funding for master's degrees and training programmes for digital sovereignty and cybersecurity using AI.
- EU funded educational programmes are advised to consider expanding their programmes adding for example new interdisciplinary topics that include security and defence and new technologies, cyber-diplomacy etc, building on existing initiatives in the framework of the European Education Area.

## 3.4 SUPPLY CHAIN SECURITY

Threat groups demonstrate a continuous interest and increased capability in supply chain attacks[173]. In 2021, ENISA assessed 24 examples of supply chain attacks which took place between January 2020 and July 2021[174]. The report reveals that **strong security protection is no longer enough for organisations when attackers have already shifted their attention to suppliers**.

ENISA discovered the following facts and figures.

- 66% of supply chain attacks focus on the supplier's code, while advanced persistent threat actors (APTs) are developing alarmingly sophisticated methodologies for approaching and overwhelming attack targets[175];
- This trend continued in 2023, as there was continued activity by threat actors making use of software update mechanisms to deliver malware to victims[176];
- An increased number of threat actors targeted identity providers, IT suppliers and managed service providers in 2023[177];
- Threat actors focus on employees as an entry point for organisations, especially targeting those with privileged access by using social engineering techniques[178];
- Supply Chain Compromise of Software Dependencies is considered the top emerging threat among the Cybersecurity threats for 2030[179].

However, supply chain security appears to be the least developed area in terms of cybersecurity risk management and NIS2 entities face a challenging task in assessing and mitigating supply chain risks. **74% of the MSs have already defined, in their national legislation, supply chain security measures for essential and important entities.** The number is expected to increase further due to the national transposition of NIS2 and the requirements of the DORA regulation for the Finance sector, which place particular emphasis on cybersecurity risk management measures offered by managed service providers.

When examining whether entities already apply such measures in 2023, it was discovered that **77% of OESs and DSPs had a policy related to supply chain cybersecurity risk management from third-parties**[180]. **However, large enterprises are more likely to have a policy (85%) compared to SMEs (53%). Even fewer entities have dedicated resources for supply chain cybersecurity.** These figures are affected by the maturity of the sector, size of the entity and the commitment of top management.

- In 2022, only 47% of the OESs and DSPs had earmarked a dedicated budget for third-party risk management[181]. Moreover, only 24% of the OESs and DSPs had dedicated employees for third-party risk management (TRM). These percentages differ between sectors. For example, third-party risk management policy is less common in digital infrastructures (55%), compared to the banking sector where 86% have such a policy in place[182].
- The percentage of OESs and DSPs with third-party risk management policies increases from 36% to 87% when management signs-off on cyber risk management measures.
- When assessing their third-party risks, 61% of the OESs and DSPs take into account whether a supplier is certified, use security risk rating services (43%) and perform due diligence or risk assessments (37%). Moreover, the entities take into account the type of product or service (59%), the volume of spending with the supplier (47%) and whether or not the supplier is subject to the NIS1 Directive (42%)[183].

Cybersecurity certification is a tool that allows product vendors and service providers to demonstrate and advertise the cybersecurity of their solutions, and for users to ensure the cybersecurity of the services and products that they acquire. **Internationally the number of schemes and assessment methodologies is growing over the years.**

- Regarding the Common Criteria scheme for ICT products, in 2024, 44% of the total assessment bodies were in Europe. This number can be explained by the SOG-IS ('Senior Officials Group Information Systems Security') Mutual Recognition agreement existing in the Union and signed by 17 MSs, which makes it possible to recognise evaluations up to the highest assurance level of the Common Criteria, and that applies a lot to sensitive ICT products such as smart cards and other hardware security modules broadly developed by EU industry[184].
- In the past few years new schemes were born to answer either sectoral needs, such as payments, telecommunications or transport, or technological needs with, for instance, the rise of connected devices[185].
- In terms of cryptographic products in the EU, the most important agreement that has dominated the EU market is the SOG-IS Agreed Cryptographic Mechanisms[186], which will be onboarded into the EUCC scheme to become the EU-wide reference for cryptographic algorithms and conformance testing for security mechanisms.

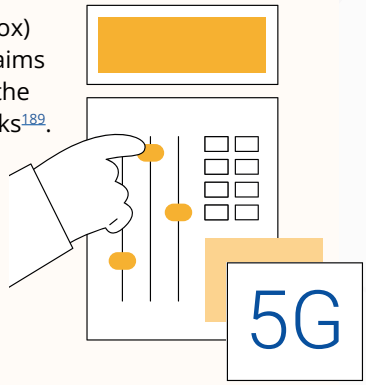
**The CRA introduces requirements for products and obligations for manufacturers that will result in more cyber secure products to be placed on the EU market.**

- 59% of the OESs and DSPs agree that common requirements would lead to a reduction in compliance costs for users as regards their supply chain.
- 56% of the OESs and DSPs agree that common requirements would lead to lower costs of risk mitigation for users.
- 61% of the OESs and DSPs agree that common requirements would reduce the number of security incidents and, as a result, the cost of managing and recovering from such incidents[187].

At EU level, the NIS2 sets out the possibility for the NIS Cooperation Group, in cooperation with the Commission and ENISA, to conduct coordinated security risk assessments of critical ICT supply chains (Article 22 of NIS2). These coordinated security risk assessments of critical ICT supply chains 'should take into account both technical and, where relevant, non-technical factors', and should follow an all hazards approach. However, in 2024, the **objective to 'improve the cybersecurity of the supply chain' was the least aligned objective among the national cybersecurity strategies of the MSs**[188].

## Good practices from Member States

The EU Toolbox on 5G cybersecurity (EU 5G Toolbox) published in January 2020 aims to address risks related to the cybersecurity of 5G networks[189]. It identifies and describes a set of strategic and technical measures, as well as corresponding supporting actions to reinforce their effectiveness, which may be put in place in order to mitigate the risks identified. MSs are currently implementing the various measures at national level on a voluntary basis.




On 9 March 2022, an informal meeting of the Telecommunications Ministers in Nevers resulted in a joint call, the so-called 'Nevers Call', to reinforce the EU's cybersecurity capabilities. It recognised that critical infrastructure such as telecommunications networks and digital services are of the utmost importance for many critical functions in our societies and are therefore a prime target for cyberattacks. The call described eight items for action, including the need to focus supply chain security on the enhancement of the resilience of communications networks, the need to strengthen the market via public-private collaboration, the rapid adoption of the NIS2 Directive and the need to build an ecosystem of trusted cybersecurity service providers.

Moreover, on 17 October 2022, the Council issued its conclusions on ICT supply chain security[190], stating that it is of utmost importance to appropriately take the geopolitical environment into consideration not only when reacting to malicious cyber activities but also when building and maintaining the resilience of information and communication technologies (ICT). The Council invited the NIS Cooperation Group, in cooperation with the Commission and ENISA, to develop a toolbox of measures for reducing critical ICT supply chain risks (ICT Supply Chain Toolbox), which is currently being developed and is expected to be ready for adoption by the end of this year.

### 3.4.1 Vulnerability handling and disclosure

According to ENISA threat landscape 2023[191], **state-nexus groups have an appetite for exploiting both old vulnerabilities and zero-day vulnerabilities.** The report highlights that there are still a lot of older vulnerabilities that can be exploited. Threat actors do not have to invest in zero-days as there are many known and unpatched vulnerabilities available for abuse. This makes the timely handling of vulnerabilities by NIS2 entities very important. In fact, according to ENISA's Foresight Cybersecurity Threats For 2030[192], the exploitation of unpatched and out-of-date systems is considered one of the top 10 emerging threats for 2030. This can be particularly significant for sectors that have a large portion of legacy systems or particularly long lifecycles for their ICT products, e.g. the energy and transport sectors.

**MSs are progressing in the definition and implementation of national coordinated vulnerability disclosure (CVD) policies.** Currently, the majority of the MSs have taken steps but they are at different levels of implementation.

- 37% of MSs have defined a national coordinated vulnerability disclosure (CVD) policy.
- 55% of MSs were currently in the process of defining such policies at the time data was being collected.
- The majority of the national vulnerability disclosure policies which are in place cover all NIS2 sectors (both essential and important entities). However, the new NIS2 sectors have the lowest coverage rate.

Vulnerability notifications are becoming more common in recent cybersecurity policy developments. For instance, NIS2, CRA, NCCS and the Regulation for EUIBAs all include mandatory or voluntary vulnerability reporting. This results in the creation of vulnerability repositories that could be leveraged to improve situational awareness.

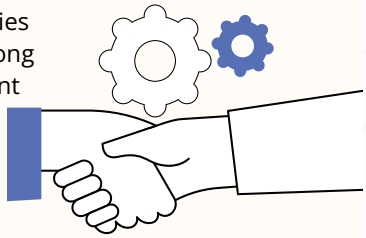
When it comes to the entities under NIS2, 'vulnerability handling and disclosure' is one of the mandatory cybersecurity risk management measures that they have to apply. This was not an explicit requirement in the NIS1 directive. Currently, **two-thirds of MSs include this measure in their national legislation. We expect more to include it as the transposition process advances.**

Regardless of whether the measure is mandatory or not, even entities that were already within the scope of NIS1 as OESs and/or DSPs face challenges in **handling vulnerabilities**. **Dealing with vulnerabilities for the entirety of their assets or patching in a timely manner are practices which, currently, are not being fully implemented and we expect this gap to grow with the addition of new sectors and entities under NIS2.** Such challenges also depend on sector characteristics.

- In 2022, 48% of the OESs and DSPs had implemented a risk-based vulnerability management process, with 26% covering only internet-facing assets and 22% only covering critical assets. Whereas 37% of the OESs and DSPs had partially implemented a risk-based vulnerability management process, it may be noted that only 15% did not have such processes at all.
- The sector with the highest share of organisations without a risk-based vulnerability management process is Online Search Engines (38%), while only 4% of the organisations in the Banking sector do not have such processes in place.
- The majority of OESs and DSPs (52%) had a rigid patching policy, in which only 20% or less of their assets are not covered. On the other hand, 13.5% of the surveyed OESs and DSPs had no visibility over the patching of 40% or more of their information assets. These can be particularly challenging for organisations with wide geographic spreads or with OT systems.
- 46% of OESs and DSPs patch critical vulnerabilities in less than a month. Furthermore, an equal percentage of the organisations surveyed indicated that they patch critical vulnerabilities within six months or less. As such, one may reasonably conclude that 92% of OESs and DSPs patch critical vulnerabilities within at least six months after their discovery. Only 8% of the organisations surveyed indicated that they exceed this time and take longer than six months to patch critical vulnerabilities in their systems.
- The transport sector is characterised by very long-life cycles for its products. In 2023, a deep dive into this sector indicated that 51% of organisations in the transport sector need one month to patch critical vulnerabilities in IT or OT assets, and 21% need a time between 1 month and six months. Only 28% of the organisations surveyed fix critical vulnerabilities on critical assets in one week.

**Good practices from Member States**

Assistance for NIS2 entities is needed to adopt a strong vulnerability management process. For example, the national competent authority can offer process templates for entities to adapt and use.



# 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.*

**To achieve this recommendation:**

- The NIS Cooperation Group, in cooperation with ENISA and the EC, could carry out systematic risk assessments of critical supply chains in the EU. These assessments could assess the risk stemming from dependencies on high-risk third-country suppliers, but they would also require significant effort and accurate data from national competent authorities.
- The EU MSs, with the support of ENISA, are encouraged to work closely with entities and specific sectors falling within the scope of the NIS2 Directive to identify ways and share good practices on managing supply chain risks, especially software dependencies. Particular focus could be placed by national competent authorities on the supervision of categories of suppliers, such as managed service providers or managed security service providers.
- In terms of vulnerability disclosure and handling, critical vulnerabilities could be monitored both at national and EU level, and across various sectors. EU MSs are advised to monitor the time for a patch to become available by a supplier, and the time needed for applying the patch by NIS2 entities. The latter could be part of the supervision mechanisms implemented by the MSs for NIS2 that refer to entities.
- Several MSs have established or are preparing national CVD policies. In this context, EU MSs could offer incentives and funding for security researchers to actively participate in CVD research, either through national or European bug bounty programmes, or through promoting and conducting cybersecurity training.
- The public sector in MSs is advised to adopt vulnerability management and disclosure policies and could share templates for other entities to use.

Chapter IV

# LOOKING AHEAD

Implementation of the NIS2 Directive, along with other key cybersecurity legislation such as the CRA and the CSOA, will increase cybersecurity capabilities across the Union. At the same time, 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. ENISA, the EU Agency for Cybersecurity, could support the EU with technical knowledge and assessments of any future possible need for targeted reviews within the existing policy framework and, especially, could support the EU in any effort aimed at mainstreaming cybersecurity robustness across EU's policies.

Still, 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**. New tasks and responsibilities do not always go hand in hand with additional resources, human, financial or otherwise, and authorities and EUIBAs are confronted with the same skill gaps affecting entities in sectors of high criticality. While short- and medium-term measures to support them may prove sufficient for the fulfilment of the responsibilities arising from new legislation, the same cannot be said with certainty about potential challenges that come with the prevalence of new technological trends and the fast-paced threat landscape.

In terms of emerging technologies, two topics have gained traction over the past year, namely AI and Post-Quantum Cryptography (PQC). In order for MSs and the EU to react promptly to the challenges arising from these new technologies, effort should be placed on technical analysis to identify the needs for, and the impact of, potential future policy interventions, as well as implications for current legislation. For example, in the field of PQC, the NIS Cooperation Group set up a dedicated workstream that aims to support and facilitate strategic cooperation and the exchange of information among MSs on the subject and that should serve as a forum to coordinate the actions of MSs at the EU level with a view to facilitating the transition to PQC by developing a roadmap, taking into account Commission Recommendation (EU) 2024/1101 of 11 April 2024. In this context, 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**. A more intense involvement in applying disruptive technologies in cybersecurity, and a forward-leaning legislative approach could bring additional benefits for the EU.

The de facto cross-border nature of cybersecurity incidents and the risks that come with it could be re-assessed in light of these 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,** not only as vehicles for cooperation and support to operators but also in terms of safeguarding their own vital operational role. In this context, 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. Developing processes for international cooperation beyond the Union would be an additional way to build up situational awareness, particularly in the case of cross-border incidents whose impact extends beyond the EU's borders. ENISA could also play a key role in this endeavour, arising from its technical credibility internationally.
The EU cybersecurity policy and legal framework is being put in place but will require time and resources to be fully implemented in order to provide the tools necessary to prepare for and respond to emerging cybersecurity challenges. It will be up to the stakeholders at national and EU level to optimise its implementation and maximise its efficiency.

Chapter V

# ANNEX

# ANNEX A: ABBREVIATIONS

| | |
|---|---|
| **AI** | Artificial intelligence |
| **AIA** | Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) |
| **CDN** | Content delivery network |
| **CER (Directive)** | Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC |
| **CISO** | Chief Information Security Officer |
| **CRA** | Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) |
| **CSA** | Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) |
| **CSIRT** | Computer security incident response team |
| **CSOA** | Cyber solidarity act |
| **CTI** | Cyber-threat intelligence |
| **CVD** | Coordinated vulnerability disclosure |
| **CyberHEAD** | Cybersecurity Higher Education Database |
| **DDoS** | Distributed denial of service |
| **DMA** | Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) |
| **DNS** | Domain name system |
| **DORA** | Regulation (EU) 2022/2554 on digital operational resilience for the financial sector |
| **DoS** | Denial of service |
| **DSA** | Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) |
| **DSP** | Digital service provider |
| **EC** | European Commission |
| **ECSF** | European Cybersecurity Skills Framework |
| **EEAS** | European External Action Service |
| **EHDS** | European health data space |

| | |
|---|---|
| **eIDAS** | Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market |
| **ENISA** | EU Agency for Cybersecurity |
| **ETL** | ENISA threat landscape report |
| **EU** | European Union |
| **EUDIF** | Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework |
| **EUCC** | European common criteria-based cybersecurity certification scheme |
| **EUIBAs** | EU Institutions, bodies and agencies of the Union |
| **Europol EC3** | Europol's European cybercrime centre |
| **FIMI** | Foreign information manipulation and interference |
| **FTE** | Full Time Equivalent |
| **ICT** | Information and communications technology |
| **IS** | Information Security |
| **ISAC** | Information Sharing and Analysis Centre |
| **IT** | Information Technology |
| **IXP** | Internet exchange point |
| **JCAR** | Joint cyber assessment report |
| **MS** | Member State |
| **NCA** | National Competent Authority |
| **NCCS** | Network Code on sector-specific rules for cybersecurity aspects of cross- border electricity flows |
| **NCSS** | National Cyber Security Strategy |
| **NIS** | Network and information security |
| **NIS CG** | Cooperation group, Art 14 of NIS 2 Directive |
| **NIS1 (Directive)** | Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union |
| **NIS2 (Directive)** | Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 1 Directive) |
| **NLO** | National Liaison Officer |
| **OES** | Operator of essential services |
| **OSINT** | Open-source intelligence |
| **OT** | Operational Technology |
| **PQC** | Post quantum cryptography |
| **R&D** | Research and development |
| **R&D&I** | Research, development and innovation |
| **RDoS** | Ransom denial of service |
| **RED (Directive)** | Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC |
| **SMEs** | Small and medium-sized enterprises |
| **SOC** | Security Operations Centre |
| **TLD** | Top-level domain |

# ANNEX B: ENISA DATA SOURCES

| SOURCE | DESCRIPTION |
|---|---|
| **EU Cybersecurity Index** | The EU Cybersecurity Index is a framework, consisting of both quantitative and qualitative indicators, to describe the cybersecurity posture of the Member States and the EU.<br><br>It serves as the core evidence base for the Report's aggregated assessment of the level of maturity of cybersecurity capabilities and resources (mandated by Article 18.1(e)). It includes an assessment of the criticality and maturity of NIS1/NIS2 sectors using both quantitative and qualitative data.<br><br>The Report only refers to EU-level data. The data set for the EU and the MSs has limited disclosure and it is not in the public domain.<br><br>The methodological framework can be found on ENISA's website: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu- cybersecurity-index |
| **Joint Cyber Assessment Report** | According to the CSA, ENISA shall prepare a regular EU Cybersecurity Technical Situation Report (JCAR) on incidents and threats based on open-source information, its own analysis and reports shared by, among others: Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact (in accordance with NIS Directive Article 14 (5)), European Cybercrime Centre (EC3) at Europol, CERT-EU.<br><br>The report has limited disclosure and is classified TLP: AMBER + STRICT. |
| **ENISA Threat Landscape** | The ENISA Threat Landscape report is the annual report of ENISA on the state of the cybersecurity threat landscape. The latest reports can be found here: https://www.enisa.europa.eu/topics/cyber-threats/threats-and- trends/?tab=publications |
| **NIS Investments Report** | This report aims at providing policy-makers with evidence to assess the effectiveness of the existing EU cybersecurity framework specifically through data on how OESs and DSPs invest their cybersecurity budgets and how the NIS Directive has influenced this investment through a large-scale survey of over 1,000 such operators.<br><br>https://www.enisa.europa.eu/publications/nis-investments-2023 |
| **Cybersecurity Higher Education Database** | The Cybersecurity Higher Education Database (CyberHEAD) is the largest validated cybersecurity higher education database in the EU and EFTA countries. It has been the main point of reference for all citizens looking to upskill their knowledge in the cybersecurity field. This list allows young talents to make informed decisions on the variety of possibilities offered by higher education in cybersecurity and helps universities attract high-quality students motivated in keeping Europe cybersecure.<br><br>https://www.enisa.europa.eu/topics/education/cyberhead |
| **ENISA Market Studies** | ENISA has developed a Cybersecurity Market Analysis Framework to scope, customise and perform market analyses. In the last few years, ENISA has analysed the market for IoT in distribution grids and for cloud cybersecurity.<br><br>https://www.enisa.europa.eu/topics/market/annual-cybersecurity-market-analyses |
| **ENISA publications on cybersecurity certification** | Based on the CSA, ENISA's certification activities are featured in a dedicated website, which also covers relevant publications.<br>For example, the report uses the ENISA Market of Cybersecurity Assessments 2018-2022:https://certification.enisa.europa.eu/publications/market-cybersecurity- assessments-2018-2022_en |
| **Foresight Cybersecurity Threats for 2030 Report** | The ENISA Foresight Cybersecurity Threats for 2030 study represents a comprehensive analysis and assessment of emerging cybersecurity threats projected for the year 2030. The study is grounded on a rigorous methodology and collaboration between experts and offers a forward-looking perspective on the evolving cybersecurity landscape.<br><br>https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030- update-2024-extended-report |

# ANNEX C: GLOSSARY OF TECHNICAL TERMS

| TERM | DESCRIPTION |
|---|---|
| **Advanced persistent threat actors (APT)** | This term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. |
| **Cybercrime / Cybercriminals** | The objective of cybercrime actors is financial gain or profits in general. Their attacks are opportunistic and indiscriminate and they target the data or infrastructure that has the highest impact on the operations of victims. They can either steal directly from victims, can extort the victim or can monetise the information stolen from victims. |
| **Cyber Threat Intelligence (CTI)** | Data and information collected and analysed to understand the threat landscape and inform decision making. |
| **Data Breach** | An intentional cyber-attack brought by a cybercriminal with the goal of gaining to unauthorised access and release sensitive, confidential or protected data. |
| **Data Leak** | An event (such as misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data. |
| **DDoS** | DDoS targets system and data availability and, though it is not a new threat, it plays a significant role in the cybersecurity threat landscape. |
| **Deepfakes** | Deepfake software can create a synthetic video or image that realistically represents anyone in the world even if they were never actually performed that action or uttered that phrase. |
| **Hacker-for-hire** | Hacker-for-hire actors contribute to the professionalisation of the cybercrime market, but also provide services to State-nexus actors. The hacker-for-hire actors can lower the barrier to get access to the criminal market, such as for example with ransomware-as-a-service or RaaS. |
| **Hacktivists** | Hacktivists are not as well-resourced as other threat actors but are often fuelled by strong motivations. Their objectives often involve disruption and they use hacking to affect some form of political or social change. The hacktivists groups are very diverse and vary heavily in skillsets and capabilities. |
| **Incident** | An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. |

# ANNEX C: GLOSSARY OF TECHNICAL TERMS

| TERM | DESCRIPTION |
|---|---|
| **Information Manipulation** | Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. |
| **Malware** | Malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system. |
| **Phishing** | A form of social engineering where attackers deceive people into revealing sensitive information. |
| **Ransomware** | A type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability or in exchange for publicly exposing the target's data. |
| **Social engineering** | Activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. |
| **State-nexus actors** | State-nexus actors, are in general well-funded, resourced and advanced. Their objective is primarily espionage and disruption, sometimes directed by the military, intelligence or state control apparatus of their country. |
| **Vulnerability** | A weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat. |
| **Wipers** | Disruptive malware designed to permanently delete or corrupt data. |
| **Zero-day vulnerability** | A vulnerability that is unknown to the organisation developing/maintaining an asset and for which no patch is available. |

# FOOTNOTES

1. https://eur-lex.europa.eu/eli/dir/2022/2555
2. See Annex B of this report.
3. http://data.europa.eu/eli/dir/2016/1148/oj.
4. http://data.europa.eu/eli/reg/2019/881/oj.
5. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
6. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32024R2847
7. https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act.
8. https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-managed-security-services-amendment.
9. http://data.europa.eu/eli/reg/2023/2841/oj.
10. http://data.europa.eu/eli/reg_impl/2024/482/oj.
11. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
12. http://data.europa.eu/eli/reg_del/2022/1645/oj.
13. http://data.europa.eu/eli/reg_impl/2023/203/oj.
14. http://data.europa.eu/eli/reg_del/2024/1366/oj.
15. http://data.europa.eu/eli/reg/2024/1183/oj.
16. http://data.europa.eu/eli/reg/2014/910/oj.
17. https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en.
18. http://data.europa.eu/eli/reg/2024/1689/oj.
19. http://data.europa.eu/eli/reg/2022/1925/oj.
20. http://data.europa.eu/eli/reg/2022/2065/oj.
21. http://data.europa.eu/eli/reg/2023/1781/oj.
22. https://eur-lex.europa.eu/eli/reg/2023/2854.
23. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
24. European Union External Action, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.
25. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
26. See https://www.eurofound.europa.eu/en/covid-19-and-digitalisation and the special Eurobarometer 532 'The Digital Decade', March 2023, available at https://europa.eu/eurobarometer/surveys/detail/2959.
27. Report on the state of the Digital Decade 2023. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade.
28. ENISA, CERT-EU, Europol (EC3), CSA Art. 7(6) Joint Cyber Assessment Report Q1,Q2,Q3 2024.
29. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
30. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
31. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
32. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
33. ENISA, CERT-EU, Europol (EC3), CSA Art. 7(6) Joint Cyber Assessment Report Q1,Q2,Q3 2024.
34. ENISA, CERT-EU, JP-23-01 - Sustained activity by specific threat actors, https://cert.europa.eu/static/files/TLP-CLEAR-JointPublication-23-01.pdf
35. One Year After: The Cyber Implications of the Russo-Ukrainian War - Sekoia.io Blog.
36. European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0380_EN.html.
37. European Union External Action, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.
38. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
39. ENISA, Foresight Cybersecurity Threats For 2030 - Update 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-204-extended-report.
40. ENISA, CERT-EU, Europol (EC3), CSA Art. 7(6) Joint Cyber Assessment Report Q1,Q2,Q3 2024.
41. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
42. Bitdefender - French Authorities Arrest Russian National - https://www.bitdefender.com/blog/hotforsecurity/french-

authorities-arrest-russian-national-allegedly-connected-to-hive-ransomware/.

43. Europol - Ragnar Locker ransomware operation taken - https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop.
44. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
45. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023.
46. Blackberry - BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows - https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows.
47. JPost - Hackers steal IDF patient records from cyberattack on Israeli hospital - https://www.jpost.com/israel-news/defense-news/article-775843.
48. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
49. ENISA, Foresight Cybersecurity Threats For 2030 - Update 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-204-extended-report.
50. ENISA, CERT-EU, Europol (EC3), CSA Art. 7(6) Joint Cyber Assessment Report Q1,Q2 2023.
51. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
52. During the analysis, incidents were identified that relate to services of sectors that are not currently within the scope of the NIS directive. These include consulting services, legal services, hospitality services etc., and are grouped under the category 'Business Services' and represent 8% of the total events.
53. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
54. ENISA, Foresight Cybersecurity Threats For 2030 - Update 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report.
55. The EU Cybersecurity Index data set has limited disclosure and it is not public. More information is available in the Annex of this report which provides an overview of data sources.
56. The indicators refer to the share of enterprises that have declared not to have suffer from such incidents.
57. The related indicator uses the terminology of NIS1.
58. On the basis of Trusted Introducer.
59. NIS2 - Article 7.
60. https://www.enisa.europa.eu/topics/national-cyber-security-strategies.
61. https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies. The report presents the situation as it was at the end of 2022.
62. These are the 17 objectives identified in ENISA's National Capabilities Assessment Framework, namely: 1. Develop a national cyber contingency plan; 2. Establish baseline security measures; 3. Secure digital identity and build trust in digital public services; 4. Organise cyber security exercises; 5. Establish an incident response capability; 6. Raise user awareness; 7. Strengthen training and educational programmes; 8. Foster R&D; 9. Provide incentives for the private sector to invest in security measures; 10. Improve the cybersecurity of the supply chain; 11. Protect critical information infrastructure, OESs and DSPs; 12. Address cybercrime; 13. Establish incident reporting mechanisms; 14. Reinforce privacy and data protection; 15. Establish a public-private partnership; 16. Institutionalise cooperation between public agencies; 17. Engage in international cooperation. For more on the assessment framework: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/. For more on the assessment framework: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/.
63. 12 out of 17 objectives are covered in the strategies of 20+ Member States.
64. Joint Statement on Log4Shell — ENISA (europa.eu).
65. ENISA Threat Landscape 2024 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 .
66. EU Toolbox on 5G Cybersecurity, NIS Cooperation Group, 29 January 2020. The EU Toolbox was adopted by the Member States' national cybersecurity authorities and endorsed by the European Council and the Commission.
67. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302841&qid=1724748319670.
68. ENISA consolidated Annual Activity Report 2023, https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2023.
69. The methodological framework can be found on ENISA's website: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index.
70. ENISA consolidated Annual Activity Report 2023; https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2023.
71. Including but not limited to the types of entities listed in Annex II of the NIS1 Directive.
72. NIS2 introduces obligations that strengthen leadership involvement in cybersecurity (Art.20).
73. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209.
74. Eurostat, European Union survey on ICT usage in households and by individuals, 2020, https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20/default/table?lang=en.
75. European Commission, Digital Decade Cardinal Points, 2023, https://digital-strategy.ec.europa.eu/en/library/cardinal-points-digital-decade-report-2023.
76. The Digital Economy and Society Index (DESI), 2022, https://digital-strategy.ec.europa.eu/en/policies/desi.
77. The Digital Economy and Society Index (DESI), 2022, https://digital-strategy.ec.europa.eu/en/policies/desi.
78. The Digital Economy and Society Index (DESI), 2022, https://digital-strategy.ec.europa.eu/en/policies/desi.
79. Eurobarometer, Special Eurobarometer 499: Europeans' attitudes towards cyber security (cybercrime), 2020, https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en.
80. Eurobarometer, Special Eurobarometer 499 : Europeans' attitudes towards cyber security (cybercrime), 2020, https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en.
81. Eurostat, European Union survey on ICT usage in households and by individuals, https://ec.europa.eu/eurostat/

databrowser/view/isoc_cisci_prv20/default/table?lang=en.

82. Eurobarometer, Special Eurobarometer 499 : Europeans' attitudes towards cyber security (cybercrime), 2020, https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en.
83. ENISA, Data based on EU-Cybersecurity Index 2024 [ind. 4b, 6], https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index/eu_csi_methodological_note_v1-0.pdf.
84. ENISA, CyberHead - Cybersecurity Higher Education Database, CYBERHEAD - Cybersecurity Higher Education Database — ENISA (europa.eu). The institutions participate in VyberHead upon interest, data is shared as obligation to be part of the tool.
85. ENISA, Cybersecurity Education Maturity Assessment, May 2024, Cybersecurity_Education_Maturity_report_en.pdf.
86. ENISA, Cybersecurity Education Maturity Assessment, May 2024, Cybersecurity_Education_Maturity_report_en.pdf.
87. ENISA, Data based on EU-Cybersecurity Index 2024, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index/eu_csi_methodological_note_v1-0.pdf.
88. ENISA, European Cybersecurity Skills Framework, https://www.enisa.europa.eu/news/developing-a-strong-cybersecurity-workforce-introducing-the-european-cybersecurity-skills-framework.
89. ENISA, CyberHEAD - Cybersecurity Higher Education Database, CYBERHEAD - Cybersecurity Higher Education Database — ENISA (europa.eu)
90. ENISA, European Cyber Security Challenge, https://ecsc.eu/about.
91. https://year-of-skills.europa.eu/index_en.
92. European Commission, Cybersecurity Skills Academy, https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.
93. https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/cybersecurity-council-approves-conclusions-for-a-more-cyber-secure-and-resilient-union/.
94. Council Conclusions on the Future of Cybersecurity: implement and protect together cybersecurity, Brussels, 21 May 2024, https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf.
95. The data sources used for the analysis in some cases concern data on NIS1 entities and in others NIS2 entities. In the case of the former, these entities will be referred to as OES/DSP whereas in the latter case as essential and important entities.
96. ENISA NIS Investment study 2023. https://www.enisa.europa.eu/publications/nis-investments-2023.
97. ENISA NIS Investment study 2023. https://www.enisa.europa.eu/publications/nis-investments-2023.
98. Source: Eurostat – European Union survey on ICT usage in enterprises. Share of enterprises using at least one of the following ICT security measures: Strong password authentication, Combination of at least two authentication mechanisms (e.g. user-defined password, one-time password (OTP), code generated via a security token or received via a smartphone, biometric methods), Encryption techniques for data, documents or e-mails, Data backup to a separate location (including backup to the cloud), Network access control (management of access by devices and users to the enterprise's network), VPN (Virtual Private Network extends a private network across a public network to enable secure exchange of data over public network), Maintenance of log files for analysis after security incidents, Performance of ICT security tests.
99. ENISA NIS Investment study 2023, https://www.enisa.europa.eu/publications/nis-investments-2023.
100. NIS2 Article 13.
101. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.
102. This finding and supporting data points below refer to the implementation of article 13.1, 13.2 and 13.3 (first data point), article 13.5 (second and third data points).
103. ENISA Data based on the EU-Cybersecurity Index, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index/eu_csi_methodological_note_v1-0.pdf.
104. Articles 13.1 and 13.2.
105. Article 13.3.
106. Directive (EU) 2022/2557 on the resilience of critical entities: https://eur-lex.europa.eu/eli/dir/2022/2557/oj.
107. NIS2 Article 13.5.
108. NIS2 Article 23.
109. eIDAS Article 19.
110. EECC Article 40.
111. It is to be noted that NIS2 Article 30 foresees the voluntary notification of (non-significant) incidents, cyber-threats and missing for important and essential entities, as well as the voluntary notification of significant incidents, cyber-threats and near misses for entities other than essential and important entities.
112. It is to be noted that NIS1, the obligation to report incidents, applies to Operators of Essential Services and Digital Service Providers (respectively under articles 14 and 16). Also, the obligation under eIDAS for trust services providers has been integrated in NIS2; Regulation (EU) 2024/1183, amending eIDAS and establishing the European Identity Framework, refers to NIS2 for incident reporting.
113. As explained in the info box, the reporting obligations for trust service providers falling under the scope of NIS2 will be driven by NIS2 provisions.
114. Network Code on Cybersecurity.
115. Commission Implementing Regulation (EU) 2023/203 on Requirements for the management of information security risks with a potential impact on aviation safety for organisations and competent authorities: https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj.
116. IS.D.OR.230 Information security external reporting scheme, included in the Commission Delegated Regulation (EU) 2022/1645 laying down rules for the application of Regulation (EU) 2018/1139 as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations.
117. https://ciras.enisa.europa.eu/ciras-visual.
118. Regulation 910/2014 (so called 'eIDAS') mandates in Article 19.2 'Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA'.
119. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Structural_business_statistics_overview#Size_class_analysis, see database: https://ec.europa.eu/eurostat/statistics-explained/images/d/d3/Structural_business_statistics_overview09-11-2023v2.xlsx.
120. Eurostat uses NACE's classification. For the purposes

of this report, we have selected the following sectors: Manufacturing, electricity, gas, steam and air conditioning supply; Water supply; Sewerage, waste management and remediation activities; Transportation and storage; Information and communication; Financial and insurance activities; Human health and social work activities. The selection is based on a rough mapping between the NIS1 sectors and NACE: as such we are aware that it can only be an imprecise estimate, which is therefore used only to give an order of magnitude. Only large enterprises were considered as, based on the ENISA NIS Investments Report 2022, large enterprises represent the largest share of the surveyed OESs and DSPs (74%).

121. Report from the Commission to the European Parliament and The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546.
122. Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C(2017) 6100 final.
123. Commission Staff Working Document – Impact Assessment Report accompanying the proposal for NIS2: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union.
124. Article 16. To know more, see: https://www.enisa.europa.eu/topics/incident-response/cyclone.
125. https://csirtsnetwork.eu/.
126. Article 9.
127. These services take place in the framework of the ENISA support action, https://www.enisa.europa.eu/publications/cybersecurity-support-action.
128. In 2023 ENISA signed working arrangements with US CISA and UA SSSCIP and UA NCSCC.
129. Even though significant advances have been made, as highlighted in section 3.1.3 Information sharing in practice: information provision, collection and exchange, the significant cybersecurity incidents reported at the EU level under specific legislation is probably only a sub-set of the incidents that actually took place.
130. ENISA Data based on the EU-Cybersecurity Index:
131. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index/eu_csi_methodological_note_v1-0.pdf.
132. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
133. ENISA NIS Investments Report 2023 - https://www.enisa.europa.eu/publications/nis-investments-2023.
134. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#:~:text=)%20and%20(isoc_cisce_ic)-,ICT%20security%20measures,access%20control%20(65%20%25.
135. Eurostat variable: E-SEC2IANY - Enterprises that experienced any ICT security related incidents leading to unavailability of ICT services, destruction or corruption of data, disclosure of confidential data (for any reason), https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en.
136. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/EDN-20230214-1.
137. The ENISA NIS Investment study 2023 indicates that 84% of the surveyed OESs and DSPs declared that they had not experienced a significant incident in 2022 and 10% did not share information about significant incidents.
138. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.
139. https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework.
140. https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map. CSIRTs of EUIBAs have not been included. Data cut-off date 09/04/2024.
141. EC Exercise Guidelines.
142. https://www.enisa.europa.eu/news/blue-olex-2023-getting-ready-for-the-next-cybersecurity-crisis-in-the-eu.
143. https://www.enisa.europa.eu/news/eu-cybersecurity-exercise-foster-cooperation-secure-free-and-fair-eu-elections.
144. https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme/cyber-europe-2024.
145. ENISA Data based on the EU-Cybersecurity Index, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index/eu_csi_methodological_note_v1-0.pdf.
146. European Commission, 2030 Report on the state of the Digital Decade, https://commission.europa.eu/europes-digital-decade-digital-targets-2030-documents_en.
147. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
148. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176,
149. ENISA NIS Investment study 2023, https://www.enisa.europa.eu/publications/nis-investments-2023,
150. ENISA NIS Investment study 2023, https://www.enisa.europa.eu/publications/nis-investments-2023,
151. SME definition, https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en,
152. ENISA NIS Investment study 2023, https://www.enisa.europa.eu/publications/nis-investments-2023,
153. ENISA Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report. https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report.
154. Eurobarometer, Cyber skills - May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
155. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
156. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
157. ENISA NIS Investment study 2023, https://www.enisa.europa.eu/publications/nis-investments-2023.
158. Eurostat study on ICT specialists in employment, May 2024, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment.
159. European Commission, Gender Equality Strategy, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/gender-equality/gender-equality-strategy_en.
160. European Commission, Women4Cyber, https://women4cyber.eu/.
161. European Commission, Women in Digital Scorecard, https://

digital-strategy.ec.europa.eu/en/news/women-digital-scoreboard-2021.

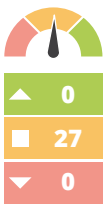
162. CONCORDIA Women in Cyber, https://www.concordia-h2020.eu/delivers/womenincyber/.
163. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
164. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
165. Eurobarometer analysis on Cyberskills, May 2024, https://europa.eu/eurobarometer/surveys/detail/3176.
166. Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises&oldid=583136#Enterprises_make_persons_employed_aware_of_their_obligations_in_ICT_security.
167. ENISA, Cybersecurity for SMEs - Challenges and Recommendations, June 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.
168. Cyber hygiene practices are addressed to two different target groups under the Directive 2022/2555: the entities (essential and important) and the citizens. See preamble 49, 89, article 7(2) points f and i, article 21(2) point g of Directive (EU) 2022/2555. The current section focuses on cyber hygiene practices addressed to entities.
169. Eurostat, European Union survey on ICT usage in enterprises, https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCE_RA/default/table.
170. Eurostat, European Union survey on ICT usage in enterprises, https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCE_RA/default/table.
171. Eurostat, European Union survey on ICT usage in enterprises, https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCE_RA/default/table.
172. https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.
173. ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
174. ENISA Threat Landscape for Supply Chain Attacks, July 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
175. ENISA Threat Landscape for Supply Chain Attacks, July 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
176. ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
177. ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
178. ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
179. ENISA Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report,
180. NIS Investments Report 2023, https://www.enisa.europa.eu/publications/nis-investments-2023,
181. NIS Investments Report 2022, https://www.enisa.europa.eu/publications/nis-investments-2022,
182. NIS Investments Report 2023, https://www.enisa.europa.eu/publications/nis-investments-2023,
183. NIS Investments 2022, https://www.enisa.europa.eu/publications/nis-investments-2022.
184. Market of Cybersecurity Assessments, ENISA, 2024, https://certification.enisa.europa.eu/publications/market-cybersecurity-assessments-2018-2022_en.
185. Market of Cybersecurity Assessments, ENISA, 2024, https://certification.enisa.europa.eu/publications/market-cybersecurity-assessments-2018-2022_en.
186. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf.
187. NIS Investments 2022, https://www.enisa.europa.eu/publications/nis-investments-2022.
188. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
189. NIS Cooperation Group, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
190. https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf.
191. ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
192. ENISA Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report.

## SMEs: Security Incidents - Disclosure of confidential data

Source: Eurostat

**What does 100 mean**

All SMEs did not experience incidents leading to disclosure of confidential data.




98,02
AVG 0,79
MAX 1,28
MIN -2,42

## CSIRTs international presence

Source: ENISA - CSIRTs by country map

**What does 100 mean**

In all EU Member States, CSIRTs are FIRST members and TI Listed /Accredited / Certified.

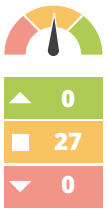

97,62
AVG 2,87
MAX 2,38
MIN -7,62

## SMEs: Security Incidents - Destruction or corruption of data

Source: Eurostat

**What does 100 mean**

All SMEs did not experience incidents leading to destruction or corruption of data.



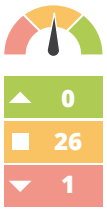

94,99
AVG 1,22
MAX 3,41
MIN -3,79

## Large enterprises: Security Incidents - Disclosure of confidential data

Source: Eurostat

**What does 100 mean**

All large enterprises did not experience incidents leading to disclosure of confidential data.



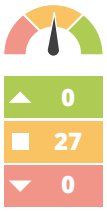

93,83
AVG 2,81
MAX 5,17
MIN -10,93

## Citizens: secure internet use

Source: Eurobarometer

**What does 100 mean**

All internet users have changed the way they use the internet due to security concerns.



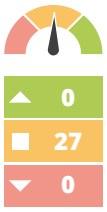

93,29
AVG 2,69
MAX 5,69
MIN -7,36

## Large enterprises: Security Incidents - Destruction or corruption of data

Source: Eurostat

**What does 100 mean**

All large enterprises did not experience incidents leading to destruction or corruption of data.



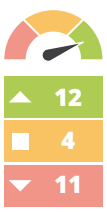

92
AVG 2,81
MAX 6,3
MIN -5,9

## Cybersecurity in R&D priorities and initiatives

Source: MS

**What does 100 mean**

All EU Member States have implemented relevant measures to support and promote cybersecurity R&D activities.




64,1
AVG 28,11
MAX 35,9
MIN -64,1

## Implementation of supervisory measures for essential and important entities

Source: MS

**What does 100 mean**

In all EU Member States, all operators in scope of NIS2 are subjected to supervisory measures by national competent authorities.


59,26
AVG 31,71
MAX 40,74
MIN -39,26

## Cybersecurity in national education curricula

Source: MS

**What does 100 mean**

All EU Member States have integrated cybersecurity curricula for primary and seconday education and updates them regularly.


58,52
AVG 25,35
MAX 41,48
MIN -58,52

## Cybersecurity graduates in higher education

Source: ENISA - CyberHead

**What does 100 mean**

The EU average reflects how EU compares to the country with the highest number of cybersecurity graduates per population in the EU.


45,65
AVG 25,7
MAX 54,35
MIN -39,48

## Coverage of vulnerability disclosure policies

Source: MS

**What does 100 mean**

In all EU Member States, vulnerabilty disclosure policies cover all NIS2 sectors of high criticality, as well the NIS2 "other critical sectors".

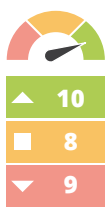

41,87
AVG 35,13
MAX 58,13
MIN -41,87

## SMEs: EU R&D funding

Source: EC - Horizon Dashboard

**What does 100 mean**

In all EU MS, SMEs have recieved all the country's EU R&D funding for cybersecurity topics within the Horizon Europe security cluster.



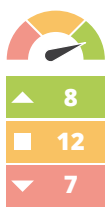

35,16
AVG 20,43
MAX 64,84
MIN -35,16

## EU R&D funding

Source: EC - Horizon Dashboard

**What does 100 mean**

In all EU MS, Cybersecurity topics have recieved all the country's EU R&D funding for the Horizon Europe security cluster.



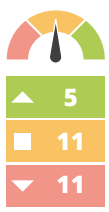

24,93
AVG 13,19
MAX 30,9
MIN -24,93

## CSIRT(s) certification

Source: ENISA - CSIRTs by country map

**What does 100 mean**

In all EU Member States, CSIRTs are TI certified.



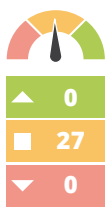

10,31
AVG 10,58
MAX 27,19
MIN -10,31

## Cybersecurity investments by essential / important entities

Source: ENISA-NIS Investments Report

**What does 100 mean**

The whole IT budget of surveyed essential/ important entities is devoted to information security.




7,14
AVG 0,54
MAX 1,46
MIN -1,24

## Enterprises: risk assessment

Source: Eurostat

**What does 100 mean**

All enterprises perform a cybersecurity risk assessment.


32,01
AVG 9,76
MAX 26,89
MIN -21,31

Catalogue number: TP-01-24-005-EN-N

## 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