enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

2026 REPORT

ON THE STATE OF CYBERSECURITY IN THE UNION

CONDENSED EDITION



COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2026

Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/).

This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union Agency for Cybersecurity, permission may need to be sought directly from the respective rightholders.

Catalogue number: TP-01-26-025-EN-N

ISBN: 978-92-9204-817-4

DOI: 10.2824/8158412

2026 Report on the State of Cybersecurity in the Union

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

EUROPEAN UNION AGENCY FOR CYBERSECURITY

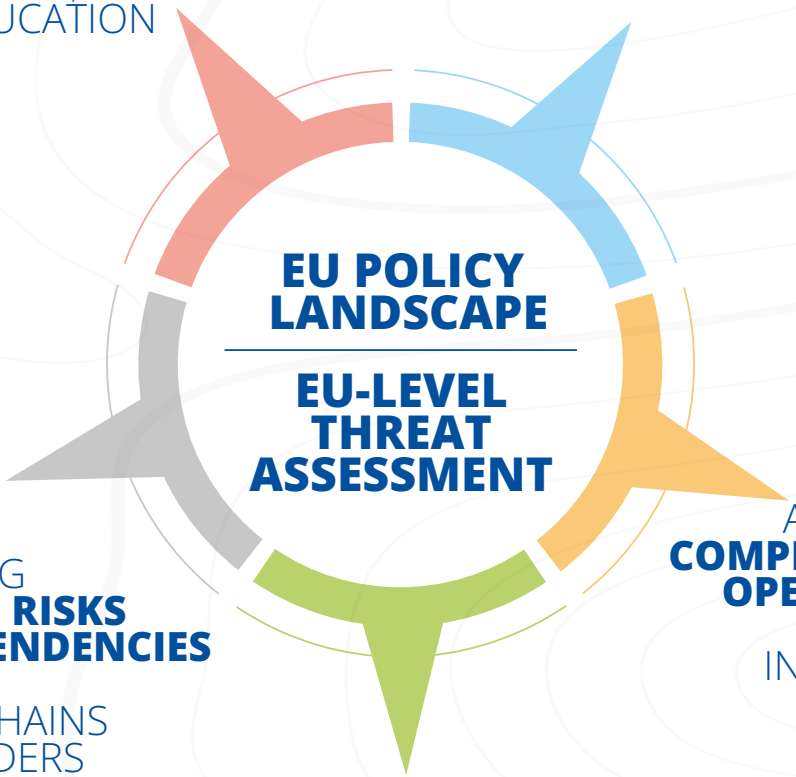
At a glance

The **Report on the State of Cybersecurity in the Union** is a biennial report that provides a regular snapshot of the state of cybersecurity from different angles: technical, legal, sectorial, and societal, while charting the trajectory of the EU for the near future.

The 2026 edition introduces a "compass", reflecting the main directions of the EU cybersecurity ecosystem. It is conceived to help stakeholders navigate the EU's evolving threat and policy landscapes. For each identified direction, it **sets out actionable policy recommendations** identifying areas for improvement.

This publication is intended to support Member States (MS) and all relevant stakeholders in their efforts to enhance the overall level of cybersecurity across the EU. The full report is available on the ENISA website.

EU Cybersecurity Ecosystem Compass



Key Takeaways



The EU's overall cybersecurity posture has improved, providing grounds for cautious confidence in times of turbulence. Acceleration of efforts is needed to maintain momentum as the threat landscape and technology evolve. Member States have greater convergence towards a high common level of cybersecurity, with most of them having achieved a mature cybersecurity posture.



The level of cyber threats to the EU is assessed as substantial. Intrusion activity remained significant and diverse throughout 2025 and in 2026, while the threat landscape is becoming more complex. Geopolitical developments continue to shape cyber activity, and financially motivated activities remain impactful. Hacktivist activity is an important component of the threat landscape. AI is increasingly acting as a force multiplier for both offensive and defensive capabilities, with advances in AI models accelerating vulnerability discovery and exploitation.



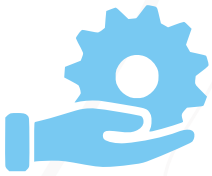
The EU policy landscape is marked by concurring trends, tackling aspects emerging from implementation, while addressing geopolitical and technological developments. As the implementation of key legislation progresses, cross-border and cross-legislative aspects are becoming increasingly relevant. This has led to an effort at legislative simplification and re-calibration. At the same time, the geopolitical context and technological developments have triggered the launch or update of several initiatives.



The maturity of critical sectors seems to be steadily improving, although unevenly across sectors. NIS2 is acting as an important catalyst for improvement. **Broader resilience strategies are becoming more important,** and a defence dimension is being introduced.



Efforts are on-going to make the EU's operational capacity in the event of crises as comprehensive as possible, including all relevant actors and towards common depiction of situational awareness. The 2025 Blueprint for Cyber Crisis Management provides a solid basis for more structured cooperation, especially among public civilian actors. Still, aspects related to the involvement and capacity of all relevant actors as well as information sharing need fine-tuning and improvement.



Supply chain risks and cross border dependencies are of growing importance to EU cybersecurity, with implications extending beyond technical aspects. The overall cybersecurity posture of a country is being increasingly determined by the cumulative level of security and trustworthiness of the goods and services on the market and their components as well as of the entities that use them. Organisations are more aware of these risks, but preparedness remains uneven.

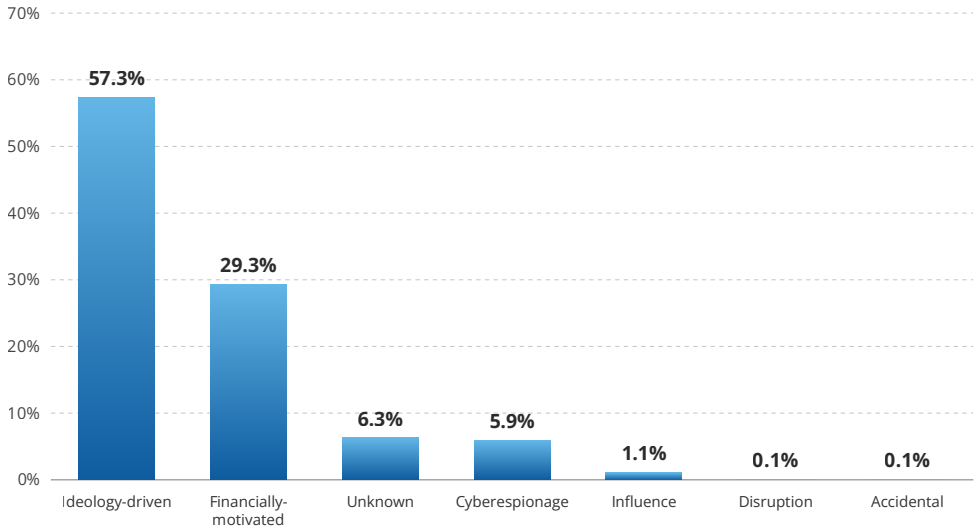


Awareness, skills and education remain fundamental to long-term resilience. There has been a shift from workforce shortage to skills shortage and AI is impacting cybersecurity profiles. These changes require sustained investment in awareness, education, recruitment, retention, and upskilling/ reskilling.

Union Level Threat Assessment

The cyber threat level to the EU during the reporting period is assessed as substantial. It is likely that entities are being directly targeted by threat actors or could be exposed to breaches using recent discovered vulnerabilities. Also, serious disruptions of essential and important entities or Union entities is considered a realistic possibility.

The threat level is the same as was reported in the 2024 Report. While this might seem surprising, given heightened geopolitical conflicts, several matters should be considered. Firstly, the threat level in 2024 already reflected activities related to Russia's war of aggression against Ukraine. Secondly, current cyber-activities related to on-going conflicts focus on the parties directly involved, despite some spillovers in the EU. Thirdly, activities affecting the EU are especially low-level distributed denial-of-service operations. These activities have a relatively low impact. The impact of AI is being assessed.



Source: ENISA Threat landscape 2026

Figure 1 - *Breakdown of incidents by assessed objectives in 2025*

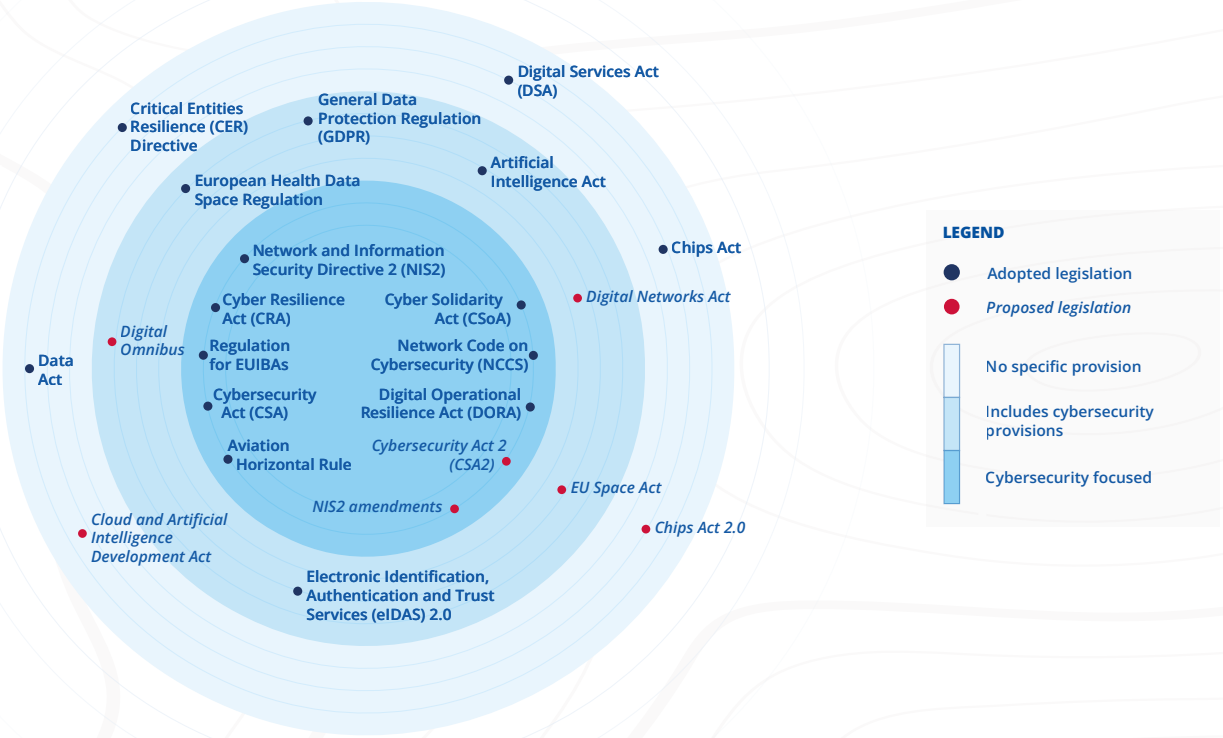
EU Policy Landscape

The EU policy landscape has been marked by concurring trends. EU, national bodies and companies have been occupied with implementing key EU cybersecurity legislation, with a focus on the NIS2 Directive.

As implementation progressed, cross-border and cross-legislative aspects have become more relevant. This has led to an effort at simplification and re-calibration, exemplified by the proposed Digital Omnibus and the NIS2 Directive targeted amendments.

The geopolitical context, technological developments and the need to make cybersecurity frameworks more agile, have triggered the launch or update of several initiatives that are relevant to cybersecurity, including the Cybersecurity Act 2 (CSA2) with a proposal for a trusted ICT supply chain security framework and the Action Plan on Cybersecurity and Artificial Intelligence.

The Cyber Resilience Act (CRA) is transitioning to operationalisation, with implementing acts, guidelines, and standards under preparation. Some obligations already apply. A delegated act is expected to establish a presumption of conformity based on the EU cybersecurity certification scheme on Common Criteria (EUCC). The Cyber Solidarity Act (CSoA), is being also operationalised, including the EU Cybersecurity Reserve, which now extends its support to Moldova and Ukraine.



The EU Cybersecurity Index

EU-level results

The overall EU average value of the Index 2026 is 71.53 points (on a scale from 0 to 100). Member States within the EU are overall aligned, with the majority of them having achieved a mature cybersecurity posture level or above. The average score of the five highest-scoring Member States is 8.33 points above the EU average, and the average score of the five lowest-scoring Member States is 11.08 points below the EU average.

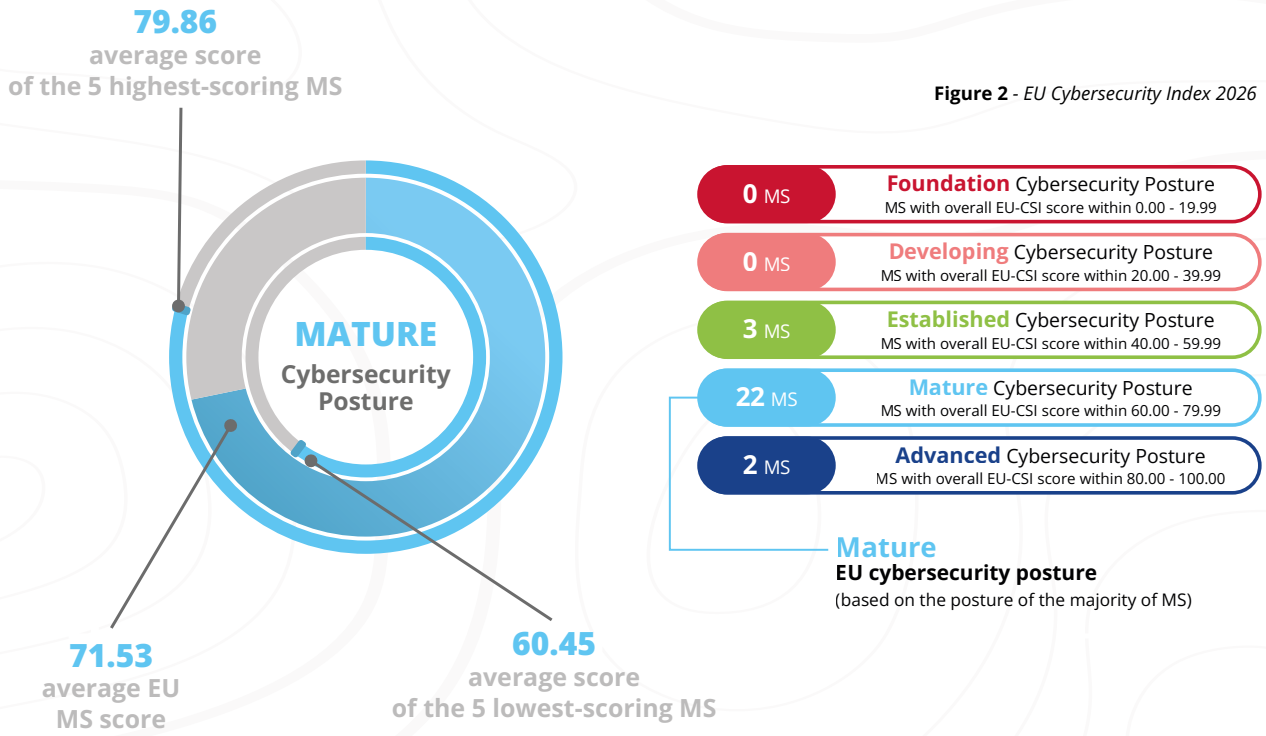


Figure 2 - *EU Cybersecurity Index 2026*

The EU Cybersecurity Index

Selected high-level findings

Policy implementation at the national level is progressing across the EU. The majority of MS achieved a mature or advanced posture on the coverage and implementation of objectives in national cybersecurity strategies (66.72 points), highlighting their increased alignment. There are, however, still gaps between strategic intent and actual execution in some areas.

Essential and important entities present a mature posture overall though there are some areas requiring improvement. Almost all MS achieved an advanced posture on practices for the management of supply chains adopted by their essential and important entities (89.91 points). Yet further improvement is possible considering the relevance of the topic. At the same time, almost all MS are at the developing level of maturity when participation by their essential and important entities in peer-to-peer information sharing activities (26.30 points) is considered. This is one of the most aligned indicators, and it shows that there is room for improvement to enhance information sharing and collaboration.

The maturity of CSIRTs still stands out as an area of potential growth. The indicator measuring the maturity level of CSIRTs is 54.76 points, and it is of the least aligned indicators, indicating that, in multiple MS, the average maturity of CSIRTs is either low or not assessed.

The presence of cybersecurity in education especially at the lower levels can be further improved. Actions to promote and enhance cybersecurity in higher levels of education are being undertaken by most MS (73.59 points), with 21 MS showcasing a mature or better posture. However, data also suggests that cybersecurity-related curricula in lower education (primary and secondary levels) is lagging behind (54.44 points) with only 12 MS achieving a mature or advanced posture.

National certification ecosystems are split between mature and less mature. The indicator on national certification capabilities shows that MS are on both edges of the maturity scale – 13 MS on the foundation or developing levels and 14 MS on the mature or advanced levels – resulting in a score in the middle of the scale (55.56 points). This is one of the least aligned indicators and it indicates that there are gaps in capabilities between MS.

Increasing coherence in the R&I landscape. Most MS achieved an advanced posture in the topic of priorities and initiatives in cybersecurity R&D (79.24 points). This indicates that the majority of MS are taking appropriate action to identify, define, promote and support cybersecurity research and development priorities both at the national and at the international level.



The process of **transposing NIS2** has been substantial and **is still ongoing**. MS are dealing with a broader set of essential and important entities than under NIS1. They are developing or expanding **supervisory governance and processes**, as well as **frameworks for risk management**, while establishing more **structured cooperation** amongst national authorities and more **structured processes for incident reporting**.

The results of these efforts are now becoming visible. More **MS** report that they will **update their lists** of relevant **important and essential entities** at least **every two years** and that they have defined a process to identify entities that are micro or small enterprises. **Risk management obligations** are now generally **in place**. Furthermore, **cooperation at the national level** and with frameworks such as DORA and CER is **mostly established**. National cybersecurity strategies show **strong alignment with NIS2 objectives**, despite some **gaps in more complex areas**, notably coordinated vulnerability disclosure (CVD), active cyber protection, mutual assistance and supply chain security.

National transpositions of NIS2 have not been fully implemented in MS and the **same scale-up in sectors** that has driven progress is also placing pressure on national competent authorities and/or bodies, **while cross-border** and **cross-legislative** aspects become more relevant.

The **variation in frameworks** for risk management and supervision among MS has an **impact on companies operating across borders**. This is true **also for incident reporting**, which is further complexified by the existence of several EU acts requiring reporting to different authorities.



The 2026 EU Cybersecurity Index indicates that most **MS have a mature approach to defining and ensuring compliance with risk management measures** for essential and important entities. MS are gradually moving towards **more formal and structured ways of checking compliance**. However, differences in security measures frameworks across MS continue to create challenges for entities operating across borders.

More **complex or newly introduced NIS2 areas** have a **lower uptake** in the action plans of National Cybersecurity Strategies, notably coordinated vulnerability disclosure (CVD), active cyber protection, mutual assistance, and supply chain security.

The **supervision of essential and important entities** is a foundational component of NIS2 implementation and is regarded as one of the **trickiest areas to operationalise**. The EU-CSI 2026 indicates persistent disparities in the share of entities for which national authorities collect at least basic information, such as names and addresses.

Different supervisory frameworks across MS and a lack of mechanisms for mutual recognition among them **affect entities operating cross-border**, as they can be subject to different rules.



The 2025 **EU Blueprint for Cyber Crisis Management** signals increased national and European commitment towards a **joint response at the EU-level to significant incidents**. Work will continue towards building a comprehensive operating environment for managing crises, whether focused on cybersecurity or with a cybersecurity component.

To this day, the EU Blueprint for cyber crisis management has never been used in a real-world situation, though **iterative testing through structured exercises** has yielded valuable insights for its operational refinement. In general, interesting national **approaches to cybersecurity exercises** are emerging and a **high participation in EU-level exercises** has been observed but it is not always matched by structured national exercises.

Collaboration among and with some actors is still under development. For example, modes of **structured cooperation with the military counterparts of EU-level networks** (such as the CSIRTs Network and EU-CyCLONe) have **not been defined yet. CSIRTs** appointed to the CSIRTs Network also show **varying maturity** levels. The role of **the private sector in crisis management is being formally recognised**. For example, it is important to exchange information about situational awareness, although this does not happen seamlessly.

The maturity of actors involved in the management of cyber crises is not equal and this **fragmented operational maturity** can represent a structural **risk to EU-wide responses** to crises. The lack of an EU-level comprehensive, common, timely depiction covering all aspects of situational awareness has persisted since the previous Report. Although trust has increased, national capacities, political, economic, policy and technical constraints remain.



The private sector plays a critical role in cyber crisis management, given its ownership and operation of much of the digital infrastructure and its early visibility of cyber threats and incidents. **Effective public-private cooperation**, including timely information sharing and clear communication channels, is **essential to strengthen situational awareness**, **coordinate responses** and **ensure business continuity**, particularly for infrastructure with cross-border impacts.

ENISA's Cyber Partnership Programme (CPP) strengthens trust and information sharing between Member States and the private sector. It facilitates **voluntary sharing of threat, incident and vulnerability information**, direct information exchange with ENISA, and ENISA-supported information sharing with **the CSIRTs Network, EU-CyCLONe and other Union entities**.

Civil-military cooperation is increasingly recognised as an important component of EU cyber crisis management, including cooperation with NATO. **The Blueprint identifies key military counterparts** and areas for cooperation, notably situational awareness and crisis management.



ADVANCING THE **RESILIENCE OF CRITICAL INFRASTRUCTURE**

Since the previous edition of this report, overall **cybersecurity maturity across critical sectors seems to be steadily improving**, along with an understanding of the specifics of the various sectors. Cybersecurity **legislation and political attention** have acted **as drivers** for investments.

Still, progress remains uneven both across and within sectors. Organisations consistently report facing **challenges in attracting and retaining cybersecurity talent**, although a few sectors are in a better position to compete for the limited talent pool available, e.g. through offering better working conditions or career development. At the same time, while **NIS2 requirements are uniform for all essential and important entities**, the **operational realities of each sector are not uniform**. Another layer of divergence emerges within the sectors themselves, particularly between large organisations and **SMEs**, which can be both more exposed and **less prepared to deal with cyberattacks** than their large counterparts.

Other factors are introducing additional considerations with regards to the resilience and preparedness of critical sectors. A **sub-set of NIS2 essential entities** will have to **comply also with CER** and take appropriate measures to ensure resilience in a broader sense. A **defence dimension is also being introduced** in the approach to **critical infrastructure**.

Finally, the speed and scale introduced by **AI-enabled threats** might translate into **increased exposure of less prepared critical organisations**, exacerbating existing differences.



While **NIS2 requirements** are uniform for all essential and important entities, the operational realities of each sector, meaning the feasibility and effort required to align with them, **is far from uniform across sectors**.

Another layer of divergence emerges within the sectors themselves, particularly **between large organisations** and **small and medium-sized entities** (SMEs). Certain **SMEs** operating in highly critical sectors are both **more exposed and less prepared to deal with cyber-attacks** than their large counterparts.



The evolution of this topic in the last two years has been exponential, driven by the increased realisation of the real-world technical and strategic impact of dependencies within and across countries. **Supply chain security**, especially when cross-border, **is a complex matter with implications extending beyond technical aspects**. In the EU market, additional **challenges** may arise **due to dependencies on foreign providers of technology**, and **exposure to strategic risks** in specific sectors, underscoring the importance of tech sovereignty.

Several tools have been designed to address the cybersecurity of supply chains. At the beginning of 2026, the NIS Cooperation Group adopted the **EU ICT Supply Chain Security Toolbox**. This provides a common, non-legally binding **framework for preparing and conducting EU-level coordinated security risk assessments of critical supply chains**. In addition, supply chain security elements embedded in EU legislation have started or continue to be implemented. In particular, **vulnerability notifications** are now more systematically **reflected in cybersecurity legislation**, including NIS2 and the Cyber Resilience Act (CRA). This is especially important as vulnerability exploitation remains a key vector for initial access and an increasing industrialisation of the discovery of vulnerabilities is being driven by frontier AI. Advances in EU legislation are accompanied by national efforts as **vulnerability disclosure policies are becoming more embedded in national cybersecurity frameworks**, although unevenly. **Developments in the EU cybersecurity certification** can also offer solutions, as reflected by the enlargement in the scope of certification to security services managed by third parties.
The **EC proposed** in January 2026, as a part of the revision of the Cybersecurity Act, **the establishment of a trusted ICT supply chain framework** to address non-technical risks related to the security the ICT supply chain. All in all, the topic is only likely to grow in importance, underscoring the necessity for the EU and MS alike to further build capacity to handle complexity.



Threat actors continue to exploit both zero-day vulnerabilities and known vulnerabilities that remain unpatched. Widespread **campaigns can now weaponise vulnerabilities within days**, and in some cases even hours or minutes, of disclosure – while **frontier AI** will also **bring down discovery time from days to hours**.

At the beginning of 2026, the NIS Cooperation Group adopted the EU ICT Supply Chain Security Toolbox, which provides a common, non-legally binding and structured approach for MS to identify, assess and mitigate the cybersecurity risks of ICT supply chains. Following an 'all-hazards approach', going beyond strictly technical aspects, it outlines risk scenarios encompassing both unintended and deliberate threats to ICT supply chains, as well as threats caused by external events and natural phenomena.

Vulnerability notification requirements are increasingly **embedded in EU** cybersecurity **legislation**, including NIS2 and the CRA. ENISA is scaling its EU Vulnerability Services and maintains the **European Vulnerability Database (EUVD)** to support Member States, CSIRTs, competent authorities and the EU internal market.

As **vulnerability handling** becomes increasingly established across the EU, the main **challenge is** no longer initial policy uptake, but achieving greater **operational maturity**, stronger **convergence** across national approaches, and more **consistent implementation** across the full vulnerability management lifecycle.



Despite some increase in digital skills, **gaps in cybersecurity awareness persist** and continue to affect a significant share of the population, suggesting that current approaches may not suffice, at least in the short term.

The **integration of cybersecurity into national educational curricula** at the primary and secondary levels **remains limited and uneven**. This is weakening resilience among future generations.

The **cybersecurity skills gap has increased**, with a perceived shift from staff to skills shortage. On the demand side, the gap is driven by the inability to find candidates as well as budget constraints. On the supply side, despite measures promoting cybersecurity in higher levels of education, **the increase in graduates has slowed down**.

While investments are key, diverse approaches such as skills attestation, competitions and bootcamps, seem to be promising ways to address the skills shortage. **Skills attestations can enhance the comparability** of professional competences, while **competitions and bootcamps can raise awareness** of cybersecurity careers and **create new pathways** into cybersecurity professions.

Finally, **AI is significantly reshaping the nature of the cybersecurity profession**. On the one hand it is reducing roles requiring repetitive analysis, on the other hand **demand is growing** for expert positions that combine cybersecurity **expertise with AI fluency**.

Work on **research and innovation** in cybersecurity is driven by academia and final **solutions have difficulties reaching the market**. Topics are driven by technological developments as well as the geopolitical and regulatory context.



Around 60% of Europeans currently have at least basic digital skills, up by approximately 5 percentage points between 2023 and 2025, against the Digital Decade **target of 80% by 2030**.

Organisations report facing **challenges in attracting and retaining talent**, although some sectors seem to be in a better position than others. On the demand side, **skills shortage** seems to be driven primarily by the inability to find candidates with the **required skills** and by **budget constraints**.

Technological **advances in Artificial intelligence (AI)** significantly **reshape the nature of the work** within cybersecurity teams.

Cybersecurity remains a specialised research field representing a **small share of EU scientific output** and dominated by academia. Limited patent activity and dedicated entrepreneurial support indicate **challenges in translating research into market-ready solutions**.

Looking Ahead

High-level policy recommendations



From rules to effective implementation

The success of EU legislation will depend to a great extent on the effectiveness of its implementation. For NIS2, building on the progress already achieved, focus should be put on **smoothening cross-border and cross-legislative aspects** so that entities operating across MS face a coherent, workable and seamless environment.



Adopting a comprehensive operational capacity in case of crisis

The 2025 Cyber Blueprint provides a solid basis for more **structured cooperation**, especially among public civilian actors. Still, aspects related to the involvement and capacity of all relevant actors, as well as **information sharing, need fine-tuning and improvement**.



Advancing the resilience of critical infrastructure

The cybersecurity of **critical infrastructure** will increasingly depend on sectors developing their maturity according to their criticality and the effectiveness with which they can **adopt broader resilience strategies**. This includes overcoming legacy limitations, maintaining operational continuity, managing supply chain risks, coping with the speed and scale introduced by **AI-enabled threats**, and dealing with increased **geopolitical volatility**.



Managing EU-level risks and dependencies across supply chains and borders

Ensuring a consistently high-level of security and reliability across borders and in the current geopolitical landscape became increasingly complex. **Cybersecurity should be coherently integrated at every step of the value and supply chain**, from secure development to secure operations.



Building long-term societal resilience: awareness, skills and education

Cybersecurity awareness and skills are a challenge for long-term resilience and require a balance of **dedicated initiatives on awareness**, **education**, **talent hiring and retention**, and **continuous upskilling and reskilling**, while considering the impact of AI.

TP-01-26-025-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.

ISBN 978-92-9204-817-4

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union