European Commission

New Cybersecurity Package

January 2026

#DigitalEU #Cybersecurity

Europe faces increasingly sophisticated hybrid attacks with a systematic cyber dimension that can disrupt critical sectors like energy, transport, health, banking and water.

The **revised Cybersecurity Act** will enable the EU to **address these security risks** while strengthening its cybersecurity.

Key Figures and Trends[1]

Global cybercrime costs: exceeded €9 trillion in 2025.

Top 5 targets in the EU: public sector, transport, digital, finance and manufacturing.

Ransomware[2]: most impactful cyber-threat in 2025; attacks every 2 seconds by 2031.

Supply chain attacks: among top 7 threats.

AI and quantum computing: significantly impacting cybersecurity.

Secure EU Information and Communication Technology (ICT) Supply Chain

The Cybersecurity Act proposes a **horizontal framework** to address security risks linked to third countries posing cybersecurity concerns.

Union-level coordinated **security risk assessments** to identify risks and vulnerabilities in specific ICT supply chains

Identification of **key assets** in the ICT supply chains

Targeted mitigation measures to address the identified risks, including prohibition to use ICT components from high-risk suppliers in key ICT assets, based on **market analysis** and thorough **economic impact assessment**

1 Source: ENISA Threat Landscape 2025 | ENISA

2 **Ransomware:** Malicious software that encrypts data or locks systems, demanding a ransom payment to restore access.

Simple and Efficient European Cybersecurity Certification Framework

The proposal simplifies certification to ensure “security-by-design”.

New possibility to **certify entities’ cyber posture** to meet market needs.

Businesses use of **certification as a tool** to enhance reputation and meet legal obligations.

Default 12-month timeline for developing schemes with streamlined procedures.

Easier Compliance with EU Cyber Rules

Clearer, simplified guidelines to help companies comply with EU cybersecurity regulations and risk management standards.

Reduce compliance costs, especially for entities operating across several Member States.

Ease compliance for 28,700 companies, including 6,200 micro and small enterprises, through targeted NIS2[3] amendments.

Harmonise application of supply chain security requirements passed from NIS2 entities to their suppliers.

Demonstrate NIS2 compliance across the EU through cyber posture certificates.

ENISA: Stronger EU Agency for Cybersecurity

The agency will enhance support for Member States and companies in anticipating, preventing, managing and responding to cyber incidents together.

Facilitate cooperation, issue early alerts and enhance situational awareness.

Operate single-entry point for incident reporting.

Set up a helpdesk with Europol and CSIRTs[4], for ransomware response and recovery.

Manage certification schemes to ensure EU products safety.

3 **NIS2 Directive:** Sets high, shared cybersecurity standards to protect our essential services.
4 **CSIRTs:** Computer Security Incident Response Teams

Publications Office of the European Union

Luxembourg: Publications Office of the European Union, 2026

PDF ISBN 978-92-68-36269-3 doi:10.2759/1925183 KK-01-26-012-EN-N

Print ISBN 978-92-68-36270-9 doi:10.2759/0583298 KK-01-26-012-EN-C