Digitalisation - European Cybersecurity Strategy

Why does it matter to intermediaries?

The **EU Cybersecurity Strategy** is an initiative aimed at building resilience to cyber threats through the Union and ensuring that citizens and businesses benefit from trustworthy digital technologies. In order to implement this strategy, the European legislators are working on several legislative proposals. The **Cyber Resilience Act** seeks to establish common cybersecurity rules for digital products and associated services that are placed on the market across the EU. The Cyber Resilience Act will complement the **Directive on measures for high common level of cybersecurity across the Union (NIS2).** The **Cyber Solidarity Act** aims to improve the preparedness, detection and response to cybersecurity incidents across the EU.

State of play

The Cyber Resilience Act

On 15 September 2022, the European Commission adopted a proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (the Cyber Resilience Act). According to the Commission hardware and software products are increasingly subject to successful cyberattacks, leading to high global annual costs of cybercrime. In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain.

Therefore, the Cyber Resilience Act aims to create conditions for the development of secure products with digital elements and create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. The proposal contains:

- Rules for placing on the market products with digital elements, to ensure their cybersecurity;
- Essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;
- Specific conformity assessment procedures for "critical products" with digital elements;
- Essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during their whole life cycle and obligations for economic operators in relation to these processes;
- Rules on market surveillance and enforcement of the above-mentioned rules and requirements.

On 31 March 2023, the Rapporteur in the ITRE Committee of the EP presented his draft report on the proposal. The Rapporteur's draft report:

- introduces an Expert Group on Cyber Resilience to support the Commission and authorities;
- adds some delay into the way critical products would have to abide by the cybersecurity certification schemes provided for in the proposal;
- requires that the money from fines collected from non-compliance with the Regulation be directed to the Digital Europe Programme.

A number of additional amendments have been presented by other MEPs and the Committee still has to adopt a final version of its draft report. In the meantime, the Council has yet to adopt its final position on the proposal before trilogue negotiations can start.

The Cyber Solidarity Act

On 18 April 2023, the Commission adopted its proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (the Cyber Solidarity Act). According to the Commission, the objective of the Cyber Solidarity Act is to support detection and awareness of cybersecurity threats and incidents, bolster preparedness of critical entities and reinforce solidarity, concerted crisis management and response capabilities across Member States.

The proposal contains the following measures:

- **Creation of a "European Cyber Shield"** comprising national and cross-border Security Operations Centres (SOCs). The objective of the Cyber Shield is to detect and act on cyber threats in a timely manner through the use of AI and advanced data analysis.
- **Creation of a "Cyber Emergency Mechanism"** aiming to increase preparedness and enhance incident response capabilities. This mechanism will notably be in charge of testing entities in highly critical sectors. It will also create a new "EU Cybersecurity Reserve" consisting of incident response services by pre-contracted trusted service providers.
- **Creation of a "Cybersecurity Incident Review Mechanism"** aiming to enhance the Union's resilience through review and assessment of significant cybersecurity incidents.

The proposal will now be examined by the EP and Council.

The Directive on measures for a high common level of cybersecurity across the Union

The Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) was adopted on 14 December 2022 and entered into force on 16 January 2023. NIS2 replaced the Directive on security of network and information systems (the NIS Directive) and improves the resilience and incident response capacities of both the public and private sector and the EU as a whole.

The NIS2 Directive is a framework containing general measures to boost cybersecurity through the EU. It applies to both public and private essential and important entities that provide their services or carry out their activities within the Union. The sectors to which the NIS2 Directive apply are listed under Annexed to the Directive and include the banking sector (and in articulation credit institutions) and the financial market infrastructures sector (and in particular operators of trading venues under MiFID II and Central Counterparties under EMIR). Insurance intermediaries and financial advisers are not mentioned in the Annexes (but this is a minimum harmonisation Directive, meaning Member States may choose to extend its scope of application).

Member States have to adopt and publish the measures necessary to comply with the NIS2 Directive by 17 October 2024, and must apply those measures from 18 October 2024.

BIPAR's position / key messages

BIPAR supports the initiative to build cyber resilience and cooperation across the Union. It highlighted on the need for the emerging frameworks to take into account pre-existing sector-specific rules (for instance the Digital Operational Resilience Act for the financial sector) in order to avoid duplication of obligations or fragmentation of the framework.

Next steps

BIPAR will continue to follow the procedures regarding the adoption of the Cyber Resilience Act and the Cyber Solidarity Act as they are examined by the EP and Council, and to assess the impact these proposals might have on our sector.

Links

- The EU Cybersecurity Strategy
- The Cyber Resilience Act
- NIS 2 Directive
- Cyber Solidarity Act
- Draft Report of the Rapporteur in the ITRE Committee
- BIPAR's website: dossier on digitalisation