ESBA Policy Briefing

EU Cyber Resilience Act (CRA)

KEY PROVISIONS

Mandatory Cybersecurity Requirements: For manufacturers, ensuring products meet essential cybersecurity standards, including risk assessments and secure default configurations.
Lifecycle Duty of Care: Continuous obligation to address vulnerabilities through security updates and testing, including after the product is in the market.
CE Marking: Products connected to the internet will bear the CE marking to indicate compliance with the CRA standards.
Scope: Applies to all products connected directly or indirectly to another device or network, excluding certain categories like open-source software, medical devices, aviation, and cars.

COMPLIANCE & ENFORCEMENT

Monitoring: Compliance will be overseen at both EU and member state levels.
Penalties: For non-compliance, substantial fines and corrective measures, including product recalls. Fines can reach up to €15 million or 2.5% of annual global turnover for manufacturers, and up to €10 million or 2% for importers and distributors.

USEFUL LINKS & RESOURCES

European Parliament Explainer
European Commission CRA web portal
EU Cyber Resilience Act Explained - EP Think Tank

INTRODUCTION

The EU Cyber Resilience Act (CRA) represents a critical step in bolstering the cybersecurity of products with digital components across the EU. Set to apply from mid-2025, the CRA aims to significantly reduce security vulnerabilities in digitally enabled products and ensure cybersecurity considerations are integral to the product lifecycle.

Enhance Cybersecurity: To safeguard consumers and businesses from cybersecurity risks associated with products or software containingm digital components.

Standardize Requirements: Establish harmonized rules for marketing products or software with digital components and set a framework of cybersecurity requirements across the product lifecycle.

IMPACT ON SMES

Cyber Risk Management: Businesses will need to conduct thorough cyber risk assessments before placing products on the market. This involves evaluating their products for security vulnerabilities and ensuring compliance with the CRA's 'essential' cybersecurity requirements.

Vulnerability Management: Ongoing management of product vulnerabilities is mandated. This includes regular testing, patch management, and clear documentation, could be resource-intensive for smaller companies

Conformity Assessment Regime: Businesses must ensure their products adhere to the conformity assessment regime. This might involve significant administrative and technical efforts, particularly for businesses with limited resources.

Incident Reporting: Manufacturers, including small enterprises, are obligated to report security events or vulnerabilities to ENISA within 24 hours of awareness. This requires small businesses to have mechanisms in place for quick detection and reporting of such incidents

European Small Business Alliance
The Independent Voice for European Entrepreneurs