The Cyber Resilience Act's silver lining: a perfect opportunity for futureproofing and trust building

February 2025

Annika Nitschke

Finding opportunities in the Cyber Resilience Act

Digital security is essential in our tech-driven world. As businesses lean more on technology, cyber threats loom larger. The EU's Cyber Resilience Act (CRA) imposes extensive obligations on businesses but also offers a golden opportunity. Weaving robust cyber security into digital products and services will not only neutralise vulnerabilities but also boost consumer trust and fortify the digital landscape for everyone.

The CRA focuses on security throughout the product lifecycle, and encourages organisations to adopt security by design, enabling them to manage cyber risks proactively and make compliance an integral part of their broader business strategy.

Who is affected by the CRA?

The CRA applies to any business involved in manufacturing or providing digital products and services in the European Union (EU). It includes any product that connects to a network or the internet. The act builds on the existing CE[1] mark, which has traditionally focused on safety but will now also include cyber-security requirements. This creates a new category of products that must carry the mark.

Manufacturers and developers of software, hardware, IoT devices, medical devices, and industrial control systems will be affected. Businesses offering software as a service (SaaS), cloud services and other network-enabled applications must also comply. Finance, healthcare and logistics (where data security is paramount) will be particularly affected.

Additionally, any company selling, importing or distributing digital products within the EU must ensure their products meet the cyber-security standards set by the CRA. This ensures all products entering the EU market adhere to uniform security guidelines.

What do companies need to do to comply?

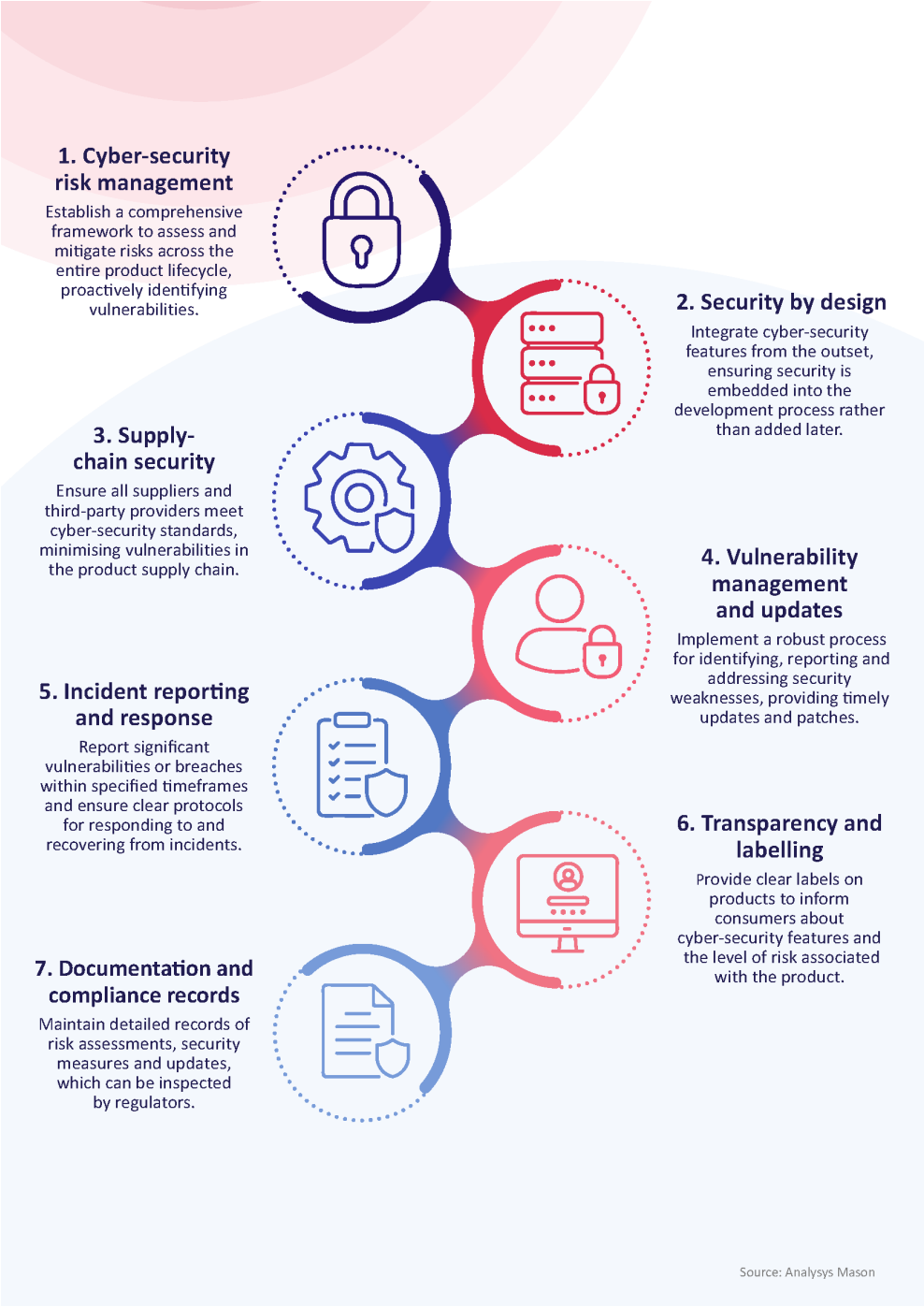
The CRA requires businesses to implement key measures to strengthen the security of their digital products, including risk management, security by design and supply-chain security (see Figure 1).

1 From the French "conformité européenne", meaning European conformity.

Companies must also manage vulnerabilities, report incidents, provide transparency through labelling, and maintain compliance records for regulators. These steps ensure products are secure throughout their lifecycle and foster consumer trust.

The CRA categorises products according to their level of criticality and significance. The specific nature of each product will dictate the type and maturity of the measures to be implemented and the type of conformity assessment, whether by an external certified body or internal self-assessment.

Figure 1: Building a stronger digital future – key requirements of the CRA



A catalyst for improvement

Compliance with the CRA offers more than just protection against fines. It fosters a cyber-security culture across the organisation, engaging all departments and aligning them towards a common goal of security and resilience. Compliance also boosts customer trust – demonstrating a commitment to data security and supporting long-term customer retention and growth.

Additionally, it safeguards brand reputation by minimising the impact of potential cyber incidents. By implementing effective risk-management practices, businesses can identify and mitigate security threats early, enhancing operational efficiency and reducing disruptions.

Moreover, compliance with the CRA can open doors to new market opportunities, allowing businesses to meet EU cyber-security standards and align with customer, partner and regulator expectations.

Support for all cyber-security levels

One of the CRA's key strengths is its ability to support businesses at various stages of cyber-security maturity – from start-ups to established enterprises. For businesses with advanced security frameworks, the CRA offers an opportunity to refine and integrate even more robust measures. For those starting their cyber-security journey, it provides a structured pathway to build a resilient security framework from the ground up.

The strategic value of cyber resilience

The CRA marks a significant step in improving digital security across Europe. While the compliance process may initially seem daunting, the long-term benefits far outweigh the challenges. Beyond regulatory compliance, the CRA enables organisations to protect their reputation, foster customer trust, and build a more secure, resilient future.

At Analysys Mason, we help businesses navigate the complexities of the CRA regardless of their maturity level. We start with comprehensive gap analyses and risk assessments to identify compliance gaps and vulnerabilities.

We then develop custom strategies, creating a clear roadmap to prioritise actions and allocate resources. For businesses launching new products, we offer expert guidance on integrating security from the outset, ensuring security by design is embedded in every phase.

Finally, we support businesses in establishing processes for continuous vulnerability management, monitoring and incident response.