CYBERSECURITY FOR BUILDING CONTROLS

Overview EU Cybersecurity Resilience Act

Contents

1. **Purpose of the Document** 2
2. **What Is the EU CRA?** 2
3. **Scope and Objectives** 2
4. **CRA-Related Roles** 2
   - 4.1. Consumer/User 2
   - 4.2. Manufacturer 2
5. **What is "Secure by Default"** 2
6. **Manufacturer responsibility for Cyber security** 3
7. **Cybersecurity requirements relating to the properties of products with digital elements** 3
8. **Manufacturers Responsibilities** 4
9. **Exception** 4
   - 9.1. Transitional provisions (§ 69) 5
   - 9.2. Exceptions for Business Users 5
10. **Relationship with Other Regulations** 5

1. Purpose of the Document

This a brief overview of the **EU Cyber Resilience Act (CRA)**. The EU Cybersecurity Resilience Act (CRA) is a regulation designed to bolster cybersecurity across the European Union by imposing mandatory requirements on products with digital elements—ranging from smart devices and industrial control systems to software platforms

2. What Is the EU CRA?

The Cyber Resilience Act (CRA) is an EU regulation designed to enhance the cybersecurity of products with digital elements—ranging from smart devices to industrial control systems. It was approved by the European Parliament on 20 March 2024 and entered into force on 10 December 2024, with full obligations applying from 11 December 2027.

3. Scope and Objectives

The Regulation establishes:

- provisions governing the placement of products with digital elements on the market to ensure their cybersecurity;
- core requirements pertaining to the design, development, and production of such products, as well as obligations for economic operators concerning cybersecurity;
- essential standards for manufacturers' vulnerability management processes to safeguard the cybersecurity of products with digital elements throughout their anticipated period of use, alongside related obligations for economic operators;
- frameworks for market surveillance, including monitoring and enforcement of the specified rules and requirements outlined in this Article.

4. CRA-Related Roles

4.1. Consumer/User

The CRA defines consumers as end users who purchase products for personal or professional use, but do not redistribute or resell them commercially. The terms "consumer" and "user" are used interchangeably.

4.2. Manufacturer

According to the CRA, a "manufacturer" is defined as a natural or legal person who develops, manufactures, or has products with digital elements designed, developed, or manufactured, and markets them under their own name or trademark, regardless of whether they are monetized or distributed free of charge.

5. What is "Secure by Default"

Manufacturers must comply with CRA standards to address cybersecurity risks during a product's entire lifecycle, including third-party components and support. Security levels and Secure by Default requirements differ based on the type of data handled:

- System data: Non-sensitive and non-critical data with no significant security or safety impact if compromised.
- Sensitive system data: Not linked to individuals, but compromise could cause notable damage or affect user safety (e.g., confidential business information, surveillance recordings).
- Personal data: Individual-related data where compromise poses minimal harm (e.g., names, public photos).
- Sensitive personal data: Individual-related data where compromise could cause significant harm (e.g., health data, private messages, financial info).
- Security data: Security-related but not individual-linked; compromising it affects product security (e.g., passwords, critical configurations).
- Critical security data: Highly sensitive, not individual-linked; integrity or confidentiality breaches can seriously impact the product and others (e.g., master keys).

Another factor is the potential attack surface and opportunity, which depend on the product's communication methods and physical accessibility. Products limited to local interfaces generally present lower security risks than those permanently connected to public networks.

“Secure by Default” refers to the practice of delivering all CE market products with adequate cybersecurity measures in place. Products containing digital elements are designed, developed, and produced to provide a level of cybersecurity that is appropriate to the assessed risks.

6. Manufacturer responsibility for Cyber security

Manufacturers are required to ensure that products with digital elements made available on the EU market comply with all applicable security requirements. This includes obligations such as conducting cybersecurity risk assessments, preparing declarations of conformity, and cooperating with relevant authorities.

Manufacturers must establish a suitable vulnerability management process to maintain the cybersecurity of digital products. Additionally, importers and distributors must fulfill specific obligations related to these processes.

Manufactures must provide consumers with clear information about the security features of both hardware and software products.

It is important to note that the requirements of the EU Cyber Resilience Act (CRA) pertain specifically to product compliance and must be met by manufacturers or any entity placing products on the EU market. The CRA does not impose direct requirements on systems or their configurations.

7. Cybersecurity requirements relating to the properties of products with digital elements

All products with digital elements must:

- Be free of known exploitable vulnerabilities when released to the market.
- Have secure default settings unless otherwise agreed with a business user.
- Allow vulnerabilities to be fixed through security updates, including automatic updates where applicable.
- Use proper controls, like authentication, to prevent unauthorized access.

- Encrypt or otherwise protect the confidentiality and integrity of data—stored, transmitted, or processed—and report any corruptions.
- Process only necessary and relevant data for their intended purpose.
- Ensure essential functions remain available even after incidents, using measures to resist denial-of-service attacks.
- Limit negative impacts on service availability for other devices or networks.
- Be designed to minimize attack surfaces and restrict unnecessary external interfaces.

Once the CRA is enforced, customers can expect all such products to demonstrate cyber resilience and be clearly notified of any cybersecurity shortcomings, even if these are deemed acceptable.

Within the EU Cyber Resilience Act (CRA), "secure by default" refers to the principle that digital products are designed and configured to be secure upon initial use, without requiring users to adjust settings significantly. For instance, it should be possible to reset a product to its original state. The original state involves deleting all local user data, restoring the software to its initial or most recent version, and returning all configurations to their default settings. The software should not include hard-coded security data or critical security information.

8. Manufacturers Responsibilities

Manufacturers of products with digital elements are required to:

- Identify and document vulnerabilities and components within those products, which includes preparing a software bill of materials in a widely used and machine-readable format that covers at least the top-level dependencies of the products.
- Address and remediate vulnerabilities promptly based on the risks to products with digital elements, including providing security updates; where technically feasible, security updates should be provided separately from functionality updates.
- Conduct regular testing and reviews of the security of products with digital elements.
- Once a security update is available, share and publicly disclose information about resolved vulnerabilities, including descriptions, product identification details, impact, severity, and clear guidance for users to address the vulnerabilities.
- Establish and enforce a policy for coordinated vulnerability disclosure.
- Implement measures that facilitate sharing information about potential vulnerabilities in their products and in third-party components, such as providing a contact address for reporting discovered vulnerabilities.
- Provide mechanisms for the secure distribution of updates for products with digital elements to ensure vulnerabilities are addressed or mitigated promptly and, where relevant for security updates, enable automatic updates.
- Ensure that security updates addressing identified issues are distributed without delay and, unless otherwise agreed with a business user for a tailor-made product, are provided free of charge along with advisory messages containing relevant information, including recommended actions for users.

9. Exception

9.1. Transitional provisions (§ 69)

Products with digital elements placed on the market before 36 months from the Regulation's start are only subject to its requirements if substantially modified afterward.

The reporting obligations apply to all relevant products with digital elements, including those already on the market.

9.2. Exceptions for Business Users

Products with digital elements must be provided with a secure default configuration, unless a manufacturer and business user agree otherwise for custom products.

10. Relationship with Other Regulations

The CRA aligns with existing EU legislation such as the **Radio Equipment Directive** and **NIS2 Directive**, ensuring harmonized standards across cybersecurity frameworks.