“Security Risks in Manufacturing Sites and Key Points You Should Know”

-European Union Cyber Resilience Act

Product Business Division HQ, Industrial Automation Business Company, OMRON Corporation

The **European Union Cyber Resilience Act (EU Cyber Resilience Act, EU-CRA)** is a regulation that establishes common cybersecurity requirements for digital products with communication capabilities placed on the EU market. Its objective is to address issues such as residual vulnerabilities in products, insufficient provision of security updates, and inadequate information disclosure to users. By doing so, the regulation aims to ensure a consistent level of security throughout the entire product lifecycle—from market placement to end-of-life—and to enhance transparency of information for users.
This publication provides an overview of the regulation and related standards, as well as an introduction to **Omron’s initiatives** in this area.

1. What is the European Union Cyber Resilience Act (EU-CRA)?

In recent years, the importance of data handled by communication-enabled devices has been increasing due to factors such as greater connectivity with external networks including the Internet, increasing complexity of supply chains, and heightened requirements for product safety and quality. At the same time, cyberattacks targeting devices within supply chains that lack sufficient security measures have been on the rise, exposing manufacturers and suppliers to the following risks:

- **Production line shutdowns and serious accidents**: Cyberattacks may result in factory control systems being compromised or information assets being leaked, potentially leading to production line stoppages, the manufacture of defective products, or serious accidents.
- **Business interruption and loss of trust**: Companies may be forced to suspend operations, suffer significant financial losses, and face legal liability, all of which can have a severe impact on business continuity.
- **Environmental pollution and health hazards**: Cyberattacks may cause the unintended release of hazardous substances, potentially resulting in environmental contamination and harm to human health.

The EU Cyber Resilience Act (EU-CRA, Regulation (EU) 2024/2847) establishes horizontal (cross-sector) cybersecurity requirements for “digital products with communication capabilities” placed on the EU market, creating a unified set of rules across the EU. The regulation is driven by several factors, including the expansion of cyberattack surfaces due to the rapid increase in connected devices, the widespread presence of vulnerabilities in products, insufficient or inconsistent provision of security updates, and the difficulty for users to obtain the information necessary to properly configure and use products—making it challenging to select and operate secure products.

The objective of the EU-CRA is not merely to make products “more secure at the time of shipment,” but to require manufacturers to continuously ensure cybersecurity support throughout the entire product lifecycle. Specifically, the regulation calls for the implementation of secure-by-design principles, the continuous provision of security updates, and greater transparency regarding support periods, thereby creating an environment in which users can take cybersecurity into account when selecting and operating products.

In addition, the EU-CRA aims to reduce legal uncertainty and the additional burden on manufacturers caused by the patchwork of cybersecurity requirements found in sector-specific regulations. By providing a framework for demonstrating conformity through the CE marking, the regulation promotes trust and facilitates smoother distribution within the EU market. As a result, procurement-side stakeholders (users) can more easily select products that offer ongoing updates and transparent information, while supply-side stakeholders (manufacturers) benefit from harmonized requirements and clearer accountability.

2. Requirements of the European Union Cyber Resilience Act (EU-CRA)

2.1. EU-CRA Requirements

The following is an overview of the requirements imposed on manufacturers under the EU Cyber Resilience Act (EU-CRA):

- **Digital products with communication capabilities** may no longer be placed on the EU (European Union) market unless they comply with the regulation by **11 December 2027**.
- **Only compliant products** are permitted to bear the **CE marking**.
- **In** the event of non-compliance, fines of up to **€15 million or 2.5% of global annual turnover**, whichever is higher, may be imposed.
- As post-market security support is mandatory, manufacturers are required to establish and maintain **continuous operational frameworks** for cybersecurity support.
- The regulation includes requirements covering **functional security requirements, secure development process requirements, vulnerability handling requirements, and product support requirements**, among others.

2.2. Schedule

- **11 December 2024**: Regulation enters into force; transition period begins
- **30 August 2026**: Publication of harmonized standards for vulnerability management requirements
- **11 September 2026**: Obligation to report actively exploited vulnerabilities to authorities begins
- **30 October 2026**: Publication of harmonized standards for Class I, Class II, and critical products
- **30 October 2027**: Publication of harmonized standards for other products
- **11 December 2027**: Regulation becomes applicable

2.3. Scope of Products and Classification

The scope of the EU-CRA covers digital products with communication capabilities, including both hardware and software. In-scope products are categorized according to their level of risk, as outlined below.

As a general principle, manufacturers are responsible for determining the product classification based on their own risk assessment. High-risk and highest risk products require third-party (Notified body) certification.

Category	内容
Basic digital products (low risk)	Digital products other than “important digital products.” These products present a relatively low level of risk, such as smart home devices and consumer IoT devices (approximately 90% of products fall into this category).

Important digital products	Class I (medium risk)	Products that may affect users' personal information or networks.
	Class II (high risk)	Products that may have a significant impact on the security of other systems or entire networks.
Critical digital products (highest risk)		Products that are deeply involved in critical national infrastructure or public safety.

2.4. Obligations of Manufacturers

Manufacturers are required not only to provide secure products, but also to establish the structures, workflows, and processes necessary to develop, deliver, and support secure products throughout their entire lifecycle. In addition, they must prepare technical documentation that demonstrate the legitimacy and appropriateness of conformity with the CU-CRA requirements, and user-facing documentation.

Items	**Overview**
Product characteristics	Products must be **designed, developed, and manufactured** to ensure an appropriate level of cybersecurity, and secure manufacturing and development processes must be implemented.
	Cybersecurity risks throughout the product lifecycle must be properly addressed, including **risk management, vulnerability handling, default security settings, security updates, maintenance and support, security notifications**, and related measures.
Vulnerability handling	**A Software Bill of Materials (SBOM)** must be created and maintained and submitted to authorities upon request.
	Security testing must be conducted and documented, and evidence must be provided to authorities upon request.
	Security updates and advisories related to vulnerabilities shall be provided free of charge. ● In providing such updates and advisories, the delivery method shall ensure protection against tampering and guarantee the authenticity of the source. ● Security updates and information related to vulnerabilities must be provided to users in a timely and appropriate manner. ● A market surveillance reporting contact point must be established. Actively exploited vulnerabilities or serious incidents must be reported to authorities in accordance with the following timelines: • Initial notification (if a significant impact is possible): within 24 hours • Detailed information: within 72 hours • Remedial actions and final report: within 14 days
Technical documentation	Documentation must be prepared and updated to demonstrate compliance with the requirements, including results of risk assessments and testing. Documentation must be retained for at least 10 years and submitted to authorities upon request.
User documentation	Information such as **manuals and guidelines**, product details, **security support periods**, and **security update methods** must be provided to users in an easy-to-understand manner.

3. Omron's Initiatives in Response to the European Union Cyber Resilience Act (EU-CRA)

3.1. Implementation of Secure-by-Design

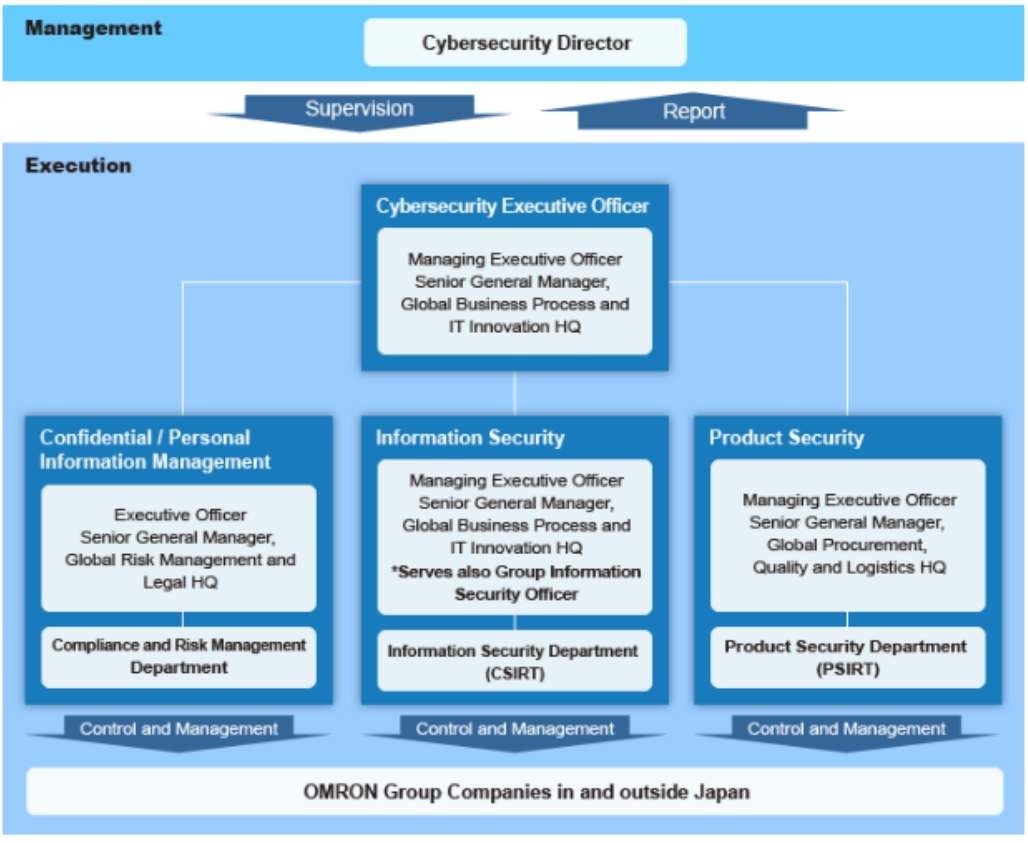
Omron has obtained third-party certification to the international standard IEC 62443-4-1, which defines process and organizational requirements for the secure development of control devices used in industrial automation and control systems. Under a secure development process compliant with this standard, Omron is advancing preparations to bring many of its factory automation (FA) products into compliance with the EU Cyber Resilience Act (EU-CRA), based on the principles of secure-by-design.

For existing products, there may be cases where adaptation to EU-CRA requirements is not feasible due to hardware or technical constraints. Taking into account each product's intended use, risk profile, implementation approach, and lifecycle, Omron is pursuing feasible mitigation measures where possible, while also considering successor products as part of its response way.

3.2. Vulnerability Handling and Cybersecurity Incident Response

To ensure the safety and peace of mind of our customers, Omron is committed to providing products and services that incorporate robust cybersecurity considerations. To support this commitment, the Omron Group as a whole is engaged in product security initiatives aimed at implementing effective countermeasures against cyberattacks.

To promote these product security activities, Omron has established a coordinated framework between its headquarters and business units**.** Within this framework, vulnerability management for products and services is handled through the Omron Product Security Incident Response Team (PSIRT[i]) structure, which has been established at both the headquarters and business unit levels to enable appropriate and timely responses.



Omron is authorized as a CVE[ii] Numbering Authority (CNA[iii]) under the CVE Program, an international initiative for managing and disclosing security vulnerabilities. This authorization allows Omron to assign CVE Identifiers (CVE IDs[iv]) independently.

As a result of obtaining CNA status, Omron is now able to assign CVE IDs internally for vulnerabilities that affect Omron Group products and services—an activity that previously required reliance on external organizations—thereby enabling more timely and efficient public disclosure of vulnerability information.

Information on vulnerabilities affecting Omron products is published on the website listed below, and the latest updates can be promptly obtained via RSS feeds.

https://www.fa.omron.co.jp/product/security/en/vulnerability/

Within Omron, we are advancing the automation of vulnerability management through the introduction of an internationally standards-compliant SBOM, and we continuously monitor vulnerabilities in the components used in our products (including OSS[v] and commercial software)

3.3. Security Guidelines

Omron publishes security guidelines with the aim of helping customers understand our cybersecurity initiatives for FA products, as well as outlining the security measures that customers are encouraged to implement when using Omron FA products. We hope that these guidelines will serve as a useful resource in supporting our customers' efforts toward EU-CRA compliance and the implementation of effective cybersecurity measures for their equipment.

https://www.fa.omron.co.jp/product/security/assets/pdf/en/P162-E1-03.pdf

4. Conclusion

This publication has provided an overview of the EU Cyber Resilience Act (EU-CRA), as well as OMRON's perspective and initiatives in response to it. We hope that the content presented herein will serve as a useful reference in supporting the security and reliability of products and equipment in the European market.

---

[i] A product security response team responsible for receiving and assessing vulnerability reports related to products, implementing remediation, disclosing information, and providing security updates.

[ii] Common Vulnerabilities and Exposures. An internationally recognized vulnerability identification framework operated by the U.S. non-profit organization MITRE Corporation.

[iii] CVE Numbering Authority. An authorized entity within the CVE Program that is permitted to assign CVE Identifiers (CVE IDs) and publish CVE records containing vulnerability information.

[iv] Vulnerabilities in software and hardware within individual products are assigned unique identification numbers, making it possible to cross-reference with information published by other organizations and to identify potential vulnerabilities.

[v] Open Source Software.