

## **CYBER RESILIENCE ACT**

### **Mitsubishi Electric's resilience management ensures CE conformity**

**The Cyber Resilience Act (CRA) requires manufacturers, importers and distributors to implement cybersecurity measures throughout the entire lifecycle of products containing digital elements. In the context of industrial automation, this means products must be developed securely from the outset ('secure by design'), delivered with preset security features ('secure by default'), and any known vulnerabilities must be actively addressed. Furthermore, free security updates must be available throughout the entire lifecycle.**

Regulation (EU) 2024/2847 was published on 20 November 2024. Reporting requirements for actively exploited vulnerabilities will take effect on 11 September 2026, with all requirements applying in full from 11 December 2027. This makes cybersecurity a central component of CE conformity.

For operators of networked production facilities, mandatory update and reporting processes will increase predictability and reduce supply chain risks. Going forward, controllers, HMIs and network technology must be

powerful, auditable and cyber-resilient. Mitsubishi Electric consistently incorporates CRA requirements into its development, operational and support processes. A Product Security Incident Response Team (PSIRT) coordinates vulnerability management and publishes countermeasures. As a CVE Numbering Authority (CNA), Mitsubishi Electric can clearly identify and communicate security vulnerabilities transparently. The company also relies on signed firmware updates, role-based access controls and monitoring concepts to protect operations and ensure compliance. All these measures are based on international standards such as IEC 62443-4-2, creating a robust foundation for auditing and verification.

**From HMI to PLC: Technical measures for auditable cyber resilience**

Mitsubishi Electric's success in implementing these requirements is well-documented. HMIs, such as the new GOT3000 series, use signed firmware updates, restrictive default configurations and role-based user management. PLC systems, such as the new MELSEC MX-F and MX-F platforms, are made resilient to cyberattacks by employing separate engineering and operating networks, encrypted remote access, and defined update processes. Typical evidence includes a complete SBOM (Software Bill of Materials), documented patch processes, log export, and communication of the support period. Comparable principles apply to drives, robots, and engineering software, including secure communication paths, documented lifecycle support periods, and disclosure of known CVEs (Common Vulnerabilities and Exposures). These measures increase resilience to manipulation and support verification in the context of CE marking.

### **Current threat situation and regulatory pressure**

Current developments highlight the relevance of CRA. According to the Dragos Report, the number of ransomware attacks on industrial organisations increased by over 87 per cent in 2024 compared to 2023, while new ICS-specific malware families were identified. At the same time, Germany is tightening requirements for companies with the NIS-2 Implementation Act. From the end of 2025 onwards, around 29,000 companies will be subject to extended security and reporting obligations, with cybersecurity explicitly becoming a management responsibility. This significantly increases compliance pressure along the industrial supply chain and supplements the CRA requirements.

### **Greater trust in industrial systems**

The CRA creates opportunities for greater transparency and trust in automation solutions. Mitsubishi Electric offers solutions for secure, future-proof production, including secure firmware updates, access controls and monitoring concepts. The company also provides checklists and security advisories to facilitate audit verification. Weekly patch windows for HMIs or PLC engineering via jump hosts according to the bastion principle are practical examples that illustrate the benefits for operations.

**Author:** Stefan Knauf, Division Manager at Mitsubishi Electric Europe B.V. Industrial Automation

### **Further information at:**

[Cyber Resilience Act CRA – Cyber security for industry](#)

## Sources

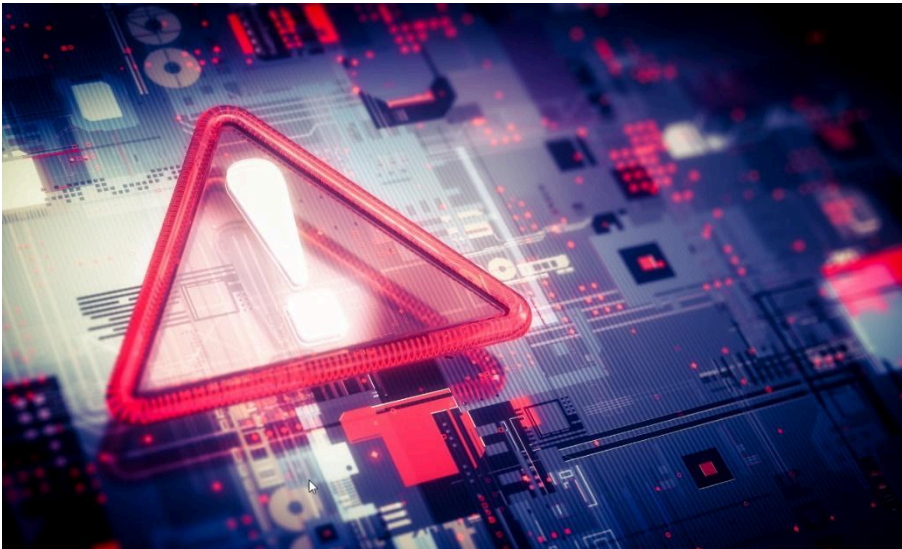
Regulation (EU) 2024/2847 \*<https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

Dragos report:

<https://www.dragos.com/resources/press-release/dragos-reports-of-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks>

NIS 2 Implementation Act: [BSI - Press - NIS 2 implementation: Bundestag passes cybersecurity law](#)

## Images



**Image 1:** Secure by default and by design. Mitsubishi Electric consistently integrates CRA requirements into development, operation, and support.

(Source: Getty Images)



**Image 2:** No chance for ransomware attacks thanks to CRA.

(Source: Getty Images)

The image(s) distributed with this press release are for editorial use only and are subject to copyright. The image(s) may only be used to accompany the press release mentioned here; any other use is prohibited.

### **About Mitsubishi Electric Corporation**

With more than 100 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognised world leader in the manufacture, marketing, and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation, and building equipment. Mitsubishi Electric enriches society with technology in the spirit of its "Changes for the Better." The company recorded a revenue of 5,521.7 billion yen (U.S.\$ 36.8 billion\*) in the fiscal year ended March 31, 2025.

For more information, please visit [www.MitsubishiElectric.com](http://www.MitsubishiElectric.com)

\*U.S. dollar amounts are translated from yen at the rate of ¥150=U.S.\$1, the approximate rate on the Tokyo Foreign Exchange Market on March 31, 2025.

### **About Mitsubishi Electric Factory Automation Business Group**

Offering a vast range of automation and processing technologies, including controllers, drive products, power distribution and control products, electrical discharge machines, electron beam machines, laser processing machines, computerised numerical controllers, and industrial robots, Mitsubishi Electric helps bring higher productivity – and quality – to the factory floor. In addition, its extensive service networks around the globe provide direct communication and comprehensive support to customers. The global slogan "Automating the World" shows the company's approach to leveraging automation for the betterment of society, through the application of advanced technology, sharing know-how, and supporting customers as a trusted partner.

For more about the story behind “Automating the World” please visit:

[www.MitsubishiElectric.com/fa/about-us/automating-the-world](http://www.MitsubishiElectric.com/fa/about-us/automating-the-world)

## Factory Automation EMEA

Mitsubishi Electric Europe B.V., Factory Automation EMEA has its European headquarters in Ratingen near Dusseldorf, Germany. It is a part of Mitsubishi Electric Europe B.V. which has been represented in Germany since 1978, a wholly owned subsidiary of Mitsubishi Electric Corporation, Japan. The role of Factory Automation EMEA is to manage sales, service, and support across its network of local branches and distributors throughout the EMEA region.

For more information, please visit [emea.mitsubishielectric.com/fa](http://emea.mitsubishielectric.com/fa)

Follow us on:



[youtube.com/user/MitsubishiFAEU](https://www.youtube.com/user/MitsubishiFAEU)



[twitter.com/MitsubishiFAEU](https://twitter.com/MitsubishiFAEU)



<https://www.linkedin.com/showcase/mitsubishi-electric-europe-factory-automation-emea/>



[https://www.instagram.com/mitsubishi\\_electric\\_fa\\_emea/](https://www.instagram.com/mitsubishi_electric_fa_emea/)

Follow us on:

**Press contact:**

**Mitsubishi Electric Europe B.V.**

Factory Automation EMEA

**Piotr Siwek**

**[Piotr.Siwek@mpl.mee.com](mailto:Piotr.Siwek@mpl.mee.com)**

**Story/Editor:**

**Andy Williams / Sam Payne**

**WPR Agency Ltd**

39 40 Calthorpe Road, Edgbaston,  
Birmingham, B15 1TS, United  
Kingdom

Tel.: +44 7880 381667

[sam.payne@wpragency.co.uk](mailto:sam.payne@wpragency.co.uk)

[www.wpragency.co.uk](http://www.wpragency.co.uk)

**Distribution/Circulation:**

**Andy Williams / Sam Payne**

**WPR Agency Ltd**

Tel.: +44 7880 381 665 / +44 7880  
381667

[andy@wpragency.co.uk](mailto:andy@wpragency.co.uk) /

[sam.payne@wpragency.co.uk](mailto:sam.payne@wpragency.co.uk)

[www.wpragency.co.uk](http://www.wpragency.co.uk)