

ei³ Releases Cyber Resilience Act Readiness Guide for Machine Builders

New guide helps OEMs prepare for CRA vulnerability handling, asset visibility, SBOM, and lifecycle cybersecurity requirements.

NEW YORK, NY, UNITED STATES, July 8, 2026 /EINPresswire.com/ -- ei³, a leader in secure industrial connectivity and Industrial Internet of Things (IIoT) solutions, has released a new educational guide to help industrial machine builders prepare for the European Union's Cyber Resilience Act (CRA).

The guide, "[Preparing for the Cyber Resilience Act: A Guide for Machine Builders](#)," explains how the CRA may affect OEMs and industrial automation suppliers as connected machines, gateways, embedded software, remote access systems, and cloud-connected applications become part of the cybersecurity attack surface.

Unlike many cybersecurity requirements that focus primarily on how organizations operate technology, the CRA places new emphasis on the security of products with digital elements. For industrial machinery builders, this creates important implications for product design, vulnerability handling, software updates, asset visibility, customer communication, and lifecycle support.

"Connected machinery is no longer static equipment once it leaves the factory," said Adam Griffen, Cybersecurity and Compliance Subject Matter Expert at ei³ and author of the guide. "As machines become more connected and software-driven, machine builders need repeatable



ei³ guide helps industrial machine builders understand Cyber Resilience Act readiness, including 2026 and 2027 deadlines, lifecycle cybersecurity, and secure remote service.

processes for identifying vulnerabilities, assessing impact, communicating with customers, and supporting remediation throughout the product lifecycle.”

The new guide outlines practical considerations for OEMs preparing for CRA-related obligations, including:

- How the CRA applies to connected industrial machinery and automation systems
- Why vulnerability handling must become a structured lifecycle process
- The role of international cybersecurity standards such as IEC 62443 and the NIST Cybersecurity Framework
- Why asset management and Software Bills of Materials (SBOMs) are becoming essential
- How [secure remote service](#) can help machine builders support remediation in the field
- Practical steps to prepare for the September 2026 and December 2027 CRA milestones

For many industrial OEMs, CRA readiness will require more than a one-time compliance review. Machines often remain in service for 10, 15, or even 20 years, and vulnerabilities may emerge long after initial deployment. The guide emphasizes that machine builders need visibility into deployed assets, a clear understanding of software and firmware components, and secure ways to support customers when updates or mitigations are required.

“

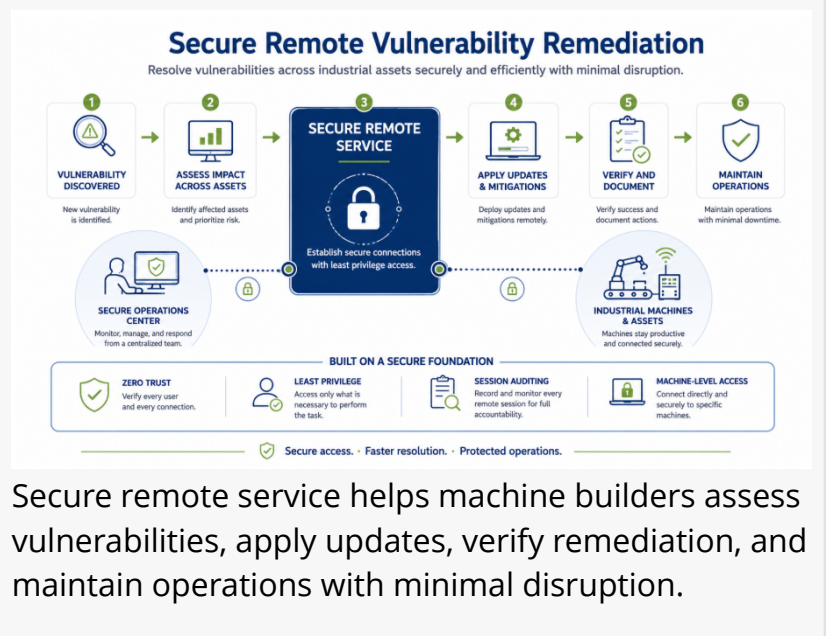
Cybersecurity is becoming a product responsibility that continues long after a machine ships.”

Spencer Cramer, CEO, ei³

“The CRA is an important signal that cybersecurity is becoming a fundamental product responsibility,” said Spencer Cramer, CEO of ei³. “For machine builders, this is not only about compliance. It is about customer trust, service readiness, and the ability to support connected machines responsibly across their operational life.”



The Cyber Resilience Act introduces new cybersecurity expectations for connected industrial machines, including vulnerability handling, asset visibility, and lifecycle support.



The guide also highlights the growing importance of secure remote service as a practical method for vulnerability remediation. In industrial environments, updates cannot always be deployed immediately or handled like traditional IT patches. Production schedules, safety requirements, customer access policies, and machine availability all affect how remediation is performed. Secure remote service can help OEMs assess issues, coordinate with customers, apply updates, verify changes, and document activity without requiring unnecessary site visits.

As global cybersecurity expectations continue to evolve, ei³ encourages machine builders to begin preparing now by strengthening visibility, vulnerability management, software inventory practices, customer communication processes, and secure lifecycle support capabilities.

The [full guide](#) is available on the ei³ website.

About ei³

ei³ is a leading provider of secure industrial connectivity, remote service, and IIoT solutions for machine builders and manufacturers. For more than 25 years, ei³ has helped OEMs and industrial enterprises connect, monitor, service, and improve machines around the world through secure, scalable, and purpose-built industrial technology.

Lauren Markofsky

ei³

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/923982519>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.