Belden

Navigating the Cyber Resilience Act:

What manufacturers, operators and asset owners need to know

White paper

By **Nils Buecker, Loic Caseras, Tobias Heer** and **André Lehmann** | Belden

Executive Summary

Digital products play a central role in industrial operations, infrastructure systems and everyday life. As connectivity increases, these devices—along with the software platforms that support them—have become attractive targets for cyberattacks.

Historically, many of these connected products were developed with a strong focus on time-to-market and new functionality, while cybersecurity practices evolved more slowly … even though **attacks are increasingly designed to target them.**

Existing laws, such as the Network and Information System 2 (NIS2) directive, the Critical Entities Resilience (CER) directive and various sector directives, have attempted to elevate cybersecurity standards and clarify responsibilities as these attacks loom. But the laws have also created a patchwork of guidance that differs based on country and product type. This makes requirements hard to interpret and compliance difficult to understand.

Given where we are with digital dependency, a horizontal regulation that provides a baseline for built-in cybersecurity across all products with digital elements is critical. This is especially true in industrial networking and OT environments, where security lags due to long lifecycles, legacy stacks and complex supply chains.

The European Union (EU) introduced the Cyber Resilience Act (CRA) in 2024 to establish **objective-oriented, technology-neutral cybersecurity requirements for consumer and industrial products.** These requirements make expectations more understandable, consistent and transparent.

The CRA doesn't replace NIS2 or other national and international sectoral regulations. Instead, it acts as a complement.

This guide will help you understand what CRA is, why it matters and what steps to take to make sure you're prepared for the changes it brings to product design, documentation and lifecycle support.

Table of Contents

What you need to know about CRA 2

CRA and NIS2: How the regulations connect 2

5 critical CRA requirements to understand 4

Taking the next steps toward CRA readiness 5

IEC 62443 as a foundation for CRA 5

Why all manufacturers must act early 5

How Belden supports CRA-ready product security 6

Preparing today for tomorrow's regulation 6

About Belden 7

What you need to know about CRA

Core elements of the Cyber Resilience Act are critical for you—whether you're a manufacturer, operator and asset owner—to understand as you design, deploy and maintain secure, compliant industrial systems.

What is CRA?

The Cyber Resilience Act is an EU regulation that introduces mandatory cybersecurity requirements for all hardware and software products with digital elements. This includes industrial products, which often blend hardware, firmware and software (including cloud connectivity and remote management). **CRA requirements apply to the product's full lifecycle, from design to end of support.**

Because these devices usually sit at the core of critical infrastructure networks, making the devices themselves more secure makes the networks they connect to more secure too.

By setting uniform, horizontal rules for products with digital elements, CRA ensures that security isn't an afterthought but a built-in condition for designing, developing and maintaining products with digital elements.

If manufacturers want to sell a product in the EU market—or if operators and asset owners want to purchase that product for use in an EU environment—then the product must meet the essential cybersecurity requirements set forth by CRA. Otherwise, the products can't be sold.

Who's affected by CRA?

The regulation applies to manufacturers that create products with digital elements for the EU market, including manufacturers of industrial networking equipment, automation equipment and associated software. It also includes original equipment manufacturers (OEMs) that produce equipment used in industrial automation and control systems.

CRA applies no matter where manufacturers are located. Vendors outside the EU that ship products into the EU market must meet CRA requirements through the importer or directly, by completing key obligations like:

- Carrying out a risk assessment
- Implementing and documenting secure development practices
- Putting structured vulnerability-handling processes in place
- Delivering lifecycle support
- Meeting any additional CRA requirements applicable

Manufacturers based in the EU that place products on the EU market are subject to the same obligations.

For manufacturers that haven't focused on cybersecurity in the past, these expectations can require significant changes. For those that have adopted frameworks to support secure development practices, the changes are often more manageable and can be addressed by extending current practices.

Operators and asset owners are affected as well: They will increasingly need CRA-compliant products when planning, purchasing and operating their systems to support regulatory and security obligations.

Which products are impacted?

CRA covers products containing software or digital logic. While not a comprehensive list, these products include:

- Firewalls and intrusion detection/prevention systems
- Routers, modems and switches
- Network management systems
- Operating systems

The regulation isn't focused on "product family" approval but applies to each unit placed on the market. Every shipped switch, router or software download must meet the requirements at the time it enters the EU market. The product classification dictates the type of approval required.

In addition, CRA expects manufacturers to manage vulnerabilities in their own code, as well as in third-party libraries and components (open-source stacks, encryption libraries, parsers or vendor SDKs) for the duration of the published support period. Otherwise, vulnerabilities in these components can render an entire product non-compliant.

How will CRA compliance be verified?

To enforce CRA rules, national market-surveillance authorities in each member state will monitor compliance through multiple channels:

- Reports from within a manufacturer's own organization
- Their own investigations and market sweeps
- Reports from other sources

CRA also weaves its requirements into the CE marking system. The CE symbol now signals that a product meets not only safety and electromagnetic compatibility (EMC) requirements but also CRA's cybersecurity expectations. Before they can affix the CE mark, manufacturers must complete CRA conformity assessments and technical documentation. Importers and distributors must check that only CRA-compliant, CE-marked products reach the EU market.

CRA and NIS2: How the regulations connect

As cybersecurity regulation tightens across Europe, CRA and NIS2 work together, with CRA focused on how products are built, and NIS2 on how products are deployed and operated.

Operators subject to NIS2 will increasingly demand CRA-ready products to meet their own obligations. Deploying equipment that doesn't meet CRA expectations could undermine security posture and regulatory compliance.

CRA will influence procurement criteria, with operators increasingly asking vendors to demonstrate CRA-aligned development processes, vulnerability handling and lifecycle support.

Together, CRA and NIS2 push cybersecurity deeper into the supply chain: Manufacturers must build secure products, and operators must select and manage those products as part of a risk-based security program.

This will mean tighter collaboration between OEMs and operators on topics like SBOM transparency, update strategies and incident communication.

5 critical CRA requirements to understand

CRA lays out several core expectations to guide manufacturers in designing, building and maintaining secure products with digital elements. They also give operators and asset owners clear assurances about the security posture of the equipment they deploy.

1. Secure by design and default

Products should be designed, developed and produced to ensure an appropriate level of cybersecurity. They must ship with secure default configurations and protections that make unsafe setups less likely and reduce common attack paths.

Core protections, such as robust authentication, cryptographic requirements, key lengths, approved algorithms, mandatory security controls, encrypted communications and hardened defaults, will be baseline expectations in many cases.

Overall, however, a risk-based approach applies: Security measures should **reflect current best practices and the state-of-the-art security level for the product.** For example, high-risk products should implement strong, extensive controls, while lower-risk products may rely on a less-stringent set of measures. This also means preparing for emerging threats by monitoring cryptographic guidance and planning for a transition to quantum-resistant algorithms as they mature and become standardized.

2. Secure development lifecycle

Manufacturers must implement a structured secure development lifecycle that covers:

- Threat and risk assessments using a structured threat-modeling approach
- Secure coding practices
- Testing and verification
- Documentation of security decisions

Aligning the development process with standards like IEC 62443-4-1 can help manufacturers meet this expectation and provide evidence of secure lifecycle practices. The standard provides a defined set of activities, documents and checkpoints that can be shown to auditors, operators or asset owners as proof that security was systematically considered throughout development.

3. Vulnerability incidents, handling and disclosure

Manufacturers must monitor, identify and remediate vulnerabilities throughout a product's lifecycle, including the detection and report of actively exploited vulnerabilities and serious incidents to authorities within defined timeframes. This process should follow a documented incident response policy that defines severity levels, response targets and escalation paths.

Manufacturers must also put processes in place to receive vulnerability reports, communicate with operators and asset owners, and provide updates without delay when issues are discovered. For example, critical vulnerabilities (defined using a standardized scoring method like the Common Vulnerability Scoring System, or CVSS) should trigger rapid assessment and initial customer notification within agreed service-level targets, followed by regular status updates and timely delivery of security fixes.

4. Lifecycle support and updates

Manufacturers must clearly communicate a defined support period to users so operators and asset owners know **how long the product will receive security fixes** and what "supported" really means.

Security updates must then be provided from product launch until the announced end of support, along with clear information about how updates will be delivered and applied.

5. Technical documentation and user information

Technical documentation serves as the internal and regulatory-facing set of records to show **how a product meets CRA's requirements** and how security is managed over its lifecycle. Internal documentation required for conformity should cover:

- Risk assessments
- Cybersecurity features
- Development and testing activities
- Vulnerability management processes

When shared externally, these technical documents should map out what operators and asset owners need to know to deploy and operate the product securely, including the product's:

- Cybersecurity characteristics
- Update mechanisms
- Support period
- Requirements for a secure configuration
- User responsibilities for maintaining security

Technical documentation and declarations of conformity must be retained so authorities can verify ongoing compliance.

Taking the next steps toward CRA readiness

To be prepared for CRA, it's time for manufacturers, operators and asset owners to formalize processes, clarify responsibilities and tighten collaboration across the supply chain.

To make compliance easier, choose partners with demonstrated industrial cybersecurity expertise, such as IEC 62443-certified development processes and established vulnerability management processes. That way, some of the heavy lifting around secure development and evidence generation will already be done on the supplier side.

Next steps for industrial product manufacturers

Before placing products on the EU market, industrial product manufacturers must be ready to:

- Conduct a conformity assessment, prepare an EU declaration of conformity covering cybersecurity. Maintain technical documentation for at least five years or the support period.
- Document clear support periods and update policies and end-of-support decisions to avoid surprises and help operators and asset owners plan lifecycle strategies.
- Develop a strategy for software bills of material (SBOMs), third-party component governance and coordinated vulnerability management across the stack, including the use of a standardized SBOM format like SPDX or CycloneDX.
- Compare current development practices to CRA expectations and frameworks, like IEC 62443-4-1 and IEC 62443-4-2, to identify gaps in secure design, testing, documentation and vulnerability handling.
- Establish or refine secure development lifecycles, SBOM generation, third-party component governance and lifecycle support policies so they can be demonstrated in a CRA conformity assessment.

Next steps for operators and asset owners

- To prepare for the impact of CRA on the supply chain, operators and asset owners should:
- Map critical systems that rely on products with digital elements and identify where CRAready products are already deployed or planned as part of modernization efforts.
- Ask suppliers questions about how they handle vulnerabilities, how long products will receive security updates, how third-party components are managed, how they're preparing for CRA timelines, whether they can provide SBOMs in a recognized format, etc.

Why all manufacturers must act early

Products cannot be placed on the market with known exploitable vulnerabilities. If they are, authorities can require corrective actions, recalls or withdrawal of products.

Early preparation reduces risk of launch delays, forced lastminute redesigns and the possibility that products can't be sold in EU markets.

New products placed on the EU market after the application date must meet the full set of requirements. Additional deadlines apply for things like reporting and how long existing products can remain available.

If manufacturers wait until those dates are close, they risk blocked launches, rushed changes and, in serious cases, penalties when obligations aren't met in time.

IEC 62443 as a foundation for CRA

Widely recognized as the reference standard for securing industrial automation and control systems, IEC 62443 can help manufacturers generate evidence and documentation to support CRA conformity assessments. Those that follow it are in a strong position to adapt to CRA regulations.

CRA aligns with:

- **IEC 62443-4-1,** which defines a secure product development lifecycle that support CRA's lifecycle obligations
- **IEC 62443-4-2,** which defines technical security requirements for components to address CRA's expectations for secure-by-design and secure-by-default products
- **IEC 62443-3-3,** which focuses on system-level security to operators integrate secure components into secure industrial networks

It's also important to recognize the limits of alignment. CRA introduces additional legal and administrative obligations, such as incident reporting, CE-marking steps, publishing support periods and documentation-retention timelines, that IEC 62443 doesn't cover. Manufacturers need to layer CRA's regulatory requirements on top of IEC 62443. communication.

How Belden supports CRA-ready product security

As a manufacturer that has a reputation for prioritizing security during product development, Belden delivers secure industrial networking products and long-term lifecycle support so they can be integrated confidently into your security programs.

We do this through a certified Secure Product Development Lifecycle, globally harmonized processes and strong security governance to help you align with CRA expectations across the product lifecycle.

Secure product development

To embed security into every stage of product creation, Belden operates a **Secure Product Development Lifecycle** across its industrial networking portfolio, aligned with IEC 62443-4-1. It covers secure design, implementation, verification and maintenance, including structured threat modeling, attack-surface analysis and risk assessments based on standardized methods like STRIDE or PASTA frameworks. Security is treated as a repeatable engineering process, not a one-off focus on individual products.

As of March 2026, **Belden holds global IEC 62443-4-1 certification with Maturity Level 4,** providing independent confirmation of our secure development practices.

Global practices across the lifecycle

To offer a consistent security experience across products and regions, Belden began rolling out its most mature IEC 62443-4-1-based development environment as a common standard for all R&D sites worldwide in 2023.

New products are **developed against a uniform security baseline** and long-term lifecycle support strategy, regardless of where they're engineered, designed or manufactured.

Connections to broader standards and governance

Beyond product-level engineering, Belden also aligns its product security work with broader information security standards, such as IEC 62443 and ISO 27001. Manufacturers, operators and asset owners can trust that device-level protections are **reinforced by organizational controls around data, processes and incident response.**

Internal governance includes central security offices and advisory roles that oversee adherence to the Secure Product Development Lifecycle and coordinate CRA-related activities, ensuring that regulatory expectations are managed consistently and cohesively.

Preparing today for tomorrow's regulation

CRA will reshape expectations for industrial networking and automation equipment. Cybersecurity will become a nonnegotiable attribute of products with digital elements.

Organizations that start aligning development processes, product portfolios and procurement policies now will be **positioned to avoid market-access issues and rushed, reactive changes later.**

By combining IEC 62443-4-1-based secure development, global process harmonization and a long-term maintenance mindset, Belden aims to support you as you navigate CRA.

Our CRA-ready products, combined with our guidance on integrating those products into secure, compliant industrial architectures over the full lifecycle, help manufacturers **reduce compliance risk and maintain a strong security posture** as requirements evolve.

Learn more

Connect to what's possible.

White paper

About Belden

Belden Inc. delivers complete connection solutions that unlock untold possibilities for our customers, their customers and the world. We advance ideas and technologies that enable a safer, smarter and more prosperous future. Throughout our 120+ year history we have evolved as a company, but our purpose remains – making connections. By connecting people, information and ideas, we make it possible. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia and Africa.

For more information, visit us at:
belden.com

follow us on

Belden