Insights, News & Events

A QUICK PRIMER TO HELP YOUR BUSINESS COMPLY WITH THE EU'S CYBER RESILIENCE ACT

Insights
Feb 24, 2026

A Quick Primer to Help Your Business Comply With the EU's Cyber Resilience Act

The European Union's Cyber Resilience Act (CRA) has mandated uniform cybersecurity requirements for hardware and software with digital elements that are placed on the EU market since 2024. The law has three main requirements: that businesses ensure their products are secure by design, that they report actively exploited vulnerabilities, and that they provide security updates for products for their expected lifetime. While the European Commission has compiled a set of technical Frequently Asked Questions to help entities comply with the law, it is voluminous and wide-ranging in scope – so this Insight summarizes the most salient topics and provides pointers for compliance.

1. What constitutes a "product with digital elements" (PDE) per the CRA, and which PDEs are in scope of the law?

CRA defines a "product with digital elements" as "a software or hardware product and its remote data processing solutions, including software and hardware components being placed on the market separately." While CRA provides technical definitions for these terms, what is most important is that there is a wide range of products that are deemed to have "digital elements," including standalone software, software paired with hardware, and hardware foundational components, consumer devices, and complex devices.

Related People

Logan S. Booth, CIPP/US
Of Counsel
720.644.2889

Daniel Pepper, CIPP/US
Partner
303.218.3661

If a product is deemed to have digital elements, it is generally within the scope of CRA if:

- it is made available on the market, and
- its intended purpose or reasonably foreseeable use include a direct or indirect logistical or physical data connection to a device or network.

In other words, most software and hardware for sale within the EU that will connect to a digital network is under the purview of CRA. Critically, the CRA only applies to PDEs placed on the market before December 11, 2027, if, from that date, they are subject to substantial modification. An exception to this rule is the notification requirement for actively exploited vulnerabilities, which applies to products placed on the market prior to December 11, 2027.

Knowing this, how can your business best understand the universe of your products that must comply with CRA?

- First, **conduct a comprehensive audit** of your full suite of PDE offerings. Determine which are sold within the EU and are likely to become part of a digital network.
- Second, **assess whether PDEs will be subject to substantial modification** *after* December 11, 2027. As an example, a software update that alters the original intended functions of the device would constitute as "substantial modification." Comparatively, an update that merely remedies a coding bug would not.
- Third, examine your product pipelines to determine which products will be controlled by CRA. Designed these products in a CRA-compliant manner from the outset.

Some products, including those designed for national security or defense and maritime equipment, fall outside the scope of CRA. You should consult with legal counsel to get a better understanding of exemptions to CRA rules.

2. What is the interplay between CRA and other related pieces of legislation?

CRA operates alongside other cybersecurity regulations. Notably, Regulation (EU) 2023/1230, known as the Machinery Regulation (MR), "addresses cybersecurity risks that may have an impact on safety," although it focuses on machinery-related items, not PDEs.

Service Focus

Data Protection and Cybersecurity

International

Privacy and Cyber

Industry Focus

Tech

Importantly, the European Commission recognizes that product classifications may not be mutually exclusive. For example, a piece of packaging machinery (covered by MR) that contains networked software and/or hardware may also be PDE covered by CRA. In this case, neither piece of legislation predominates. Instead, businesses must ensure that they follow both MR and CRA, especially since complying with one law may reinforce compliance with the other.

For those businesses whose products may be governed concurrently by CRA and other EU regulations (e.g., MR, General Data Protection Regulation, General Product Safety Regulation, etc.), the following guidance is applicable:

- Initiate a review of all products that you have placed into the EU market. You should classify each product, understanding that some may have multiple designations.
- Consult with legal counsel to see what EU laws apply to which products and to help reconcile seemingly conflicting regulations.
- Reference applicable conformity assessment procedures set forth by the EC, which are designed to help facilitate compliance across multiple regulatory regimes.

3. What does CRA require in terms of the manufacturer's cybersecurity risk assessment?

Before introducing a PDE to market, CRA "requires manufacturers to undertake an assessment of the cybersecurity risks associated with a product with digital elements." The goal of this assessment is to minimize cybersecurity risks, prevent incidents, and minimize their impact, including in relation to the health and safety of users.

The cybersecurity risk assessment must indicate certain information, including:

- Whether (and, if so, how) the security requirements of CRA are applicable to the PDE;
- The way those requirements are being implemented by the business;
- How the manufacturer has planned, designed, developed, produced, delivered and maintained the PDE to ensure an

appropriate level of cybersecurity; and

- The vulnerability handling requirements.

CRA does not mandate a specific cybersecurity risk assessment methodology, so a manufacturer can decide how to identify and treat the relevant risks. However, this process must be comprehensive, as all relevant risks must be addressed, and this process needs to be documented so that regulators can verify compliance.

The most effective way to comply with this provision of CRA is for the manufacturer to consult with legal and technical experts who can validate that the cybersecurity risk assessment meets regulatory standards, and that the process undertaken by the business has been thorough and covered all necessary requirements.

4. What reporting requirements must a manufacturer meet upon discovery of an actively exploited vulnerability or a severe incident?

A key provision of CRA is the reporting of actively exploited vulnerabilities (defined as "a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner") and severe incidents to regulators.

CRA does not provide an exhaustive list as to how a manufacturer may become aware of an actively exploited vulnerability, but some examples include the following:

- A customer or partner relaying unusual activity or compromise;
- A threat intelligence report, government agency, and/or ethical hacker that advises that the manufacturer's product has been used in targeted attacks; or
- Internal monitoring, scanning activities, and/or telemetry.

Where CRA is prescriptive is that once an actively exploited vulnerability is discovered, it must be reported. Best practices to meet reporting requirements include:

- Draft templated forms that can be filled with applicable information *before* a vulnerability is discovered. These forms should include all information required by CRA and be vetted by attorneys.

- Institute an approval process for forms to be expeditiously routed, reviewed, and signed off for filing. Identifying who will draft the form, what personnel need to review it, and the individual ultimately responsible streamlines the process.
- Consult with counsel to keep abreast of any changes to the disclosures and/or filing procedures. Agencies sometimes evolve what information they need or how a form should be submitted, and your attorneys should help you be aware of any such developments.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Data Protection and Cybersecurity Team.