Nemko Digital

CRA: Are You Ready for September 2026? Webinar Report

Executive Summary

This report summarizes the "Getting Ready for September 11" webinar hosted by Nemko Digital on July 7, 2026. The webinar focused on the upcoming European Union Cyber Resilience Act (CRA), a significant piece of legislation aimed at improving the cybersecurity of products with digital elements. The speakers provided a comprehensive overview of the CRA's scope, key deadlines, specific requirements for vulnerability handling and incident reporting, and actionable steps for organizations to achieve compliance.

Main Theme and Objectives

The primary theme of the webinar was preparing manufacturers and relevant stakeholders for the fast-approaching compliance deadlines of the EU Cyber Resilience Act, specifically the mandatory vulnerability and incident reporting requirements taking effect on September 11, 2026. The objectives were to:

1.Clarify the scope of the CRA and what constitutes a "product with digital elements."

2.Detail the specific obligations and strict timelines for vulnerability and incident reporting.

3.Outline the necessary documentation and processes required for compliance.

4.Provide a strategic roadmap for organizations to begin their compliance journey.

Key Segments and Discussions

1. Introduction to Nemko Digital and the CRA Scope

Nemko Digital

Pep van der Laan opened the session by introducing Nemko Digital's role in supporting organizations with digital compliance, focusing on advisory services, regulatory compliance (including the AI Act and CRA), and AI trust.

He then provided a high-level overview of the CRA, emphasizing that it aims to reduce vulnerabilities in products with digital elements by enforcing security by design and default. Crucially, the scope extends beyond just hardware to include:

- Hardware Devices: The physical product itself.
- Software: Both embedded software and supporting applications.
- Remote Data Processing Solutions: Cloud services, APIs, or backend systems that are essential to the product's functioning.

The CRA establishes a lifecycle responsibility for manufacturers, covering design, sourcing (supply chain), development, production, and a defined support period after the product is placed on the market.

2. Important Deadlines and Connections to Other Regulations

The webinar highlighted two critical deadlines:

- September 11, 2026: Mandatory vulnerability disclosure and incident reporting obligations begin.
- December 11, 2027: Full compliance with all CRA requirements is mandatory for products sold in the EU.

Van der Laan also discussed how the CRA interacts with other frameworks. For instance, while the Radio Equipment Directive (RED) includes some cyber requirements, the CRA's requirements are broader and will eventually supersede them. Furthermore, compliance with the CRA provides a presumption of conformity for the cybersecurity requirements outlined in the EU AI Act.

3. Deep Dive: Vulnerability and Incident Reporting (The September 11 Deadline)

Gustavo Sánchez detailed the specific reporting obligations taking effect in September 2026. He outlined the strict timelines manufacturers must adhere to once they become aware of an actively exploited vulnerability or a severe incident:

- 24 Hours: An early warning must be submitted.

- 72 Hours: A more detailed notification, including an initial assessment, is required.
- 14 Days (for vulnerabilities): A final report detailing corrective measures and mitigations.
- 1 Month (for incidents): A final report encompassing due diligence and forensics.

Sánchez emphasized that the "clock starts ticking" not when a vulnerability is merely submitted via a form, but after an initial triage and validation process confirms its severity or active exploitation.

4. Required Capabilities and Documentation

To meet these reporting obligations, organizations must establish robust internal capabilities:

- Coordinated Vulnerability Disclosure (CVD): A structured framework allowing external researchers and ethical hackers to report vulnerabilities anonymously and securely.
- Documentation and Record Keeping: Manufacturers must maintain detailed records ensuring traceability, testability, and treatability of vulnerabilities. This includes identifiers, status, risk levels (likelihood x impact), and root causes. By 2027, this will also require linking vulnerabilities to Software Bill of Materials (SBOMs).
- Single Reporting Platform (SRP): Reporting will be centralized through the ENISA Single Reporting Platform, which will route information to the relevant national Computer Security Incident Response Teams (CSIRTs).

5. Getting Started: The Path to Compliance

Van der Laan concluded the presentation segment by offering a practical approach for organizations to start their compliance efforts. Given the tiered structure of the CRA (categorizing products into Default, Important, and Critical), the foundational step is conducting a Cyber Risk Assessment. Understanding the specific cyber risks associated with a product dictates the necessary controls and the path to conformity (e.g., self-declaration for default products vs. third-party assessment for critical ones).

Nemko Digital

Q&A Session Highlights

The webinar concluded with a Q&A session addressing participant concerns:

- Software vs. Hardware: It was clarified that standalone software can qualify as a product with digital elements and fall under the CRA's scope, even without a specific hardware component.
- Remote Data Processing: Elements like cloud services, APIs, and telemetry portals are in scope if the product relies on them to function.
- Relationship with Machinery Regulation: While the Machinery Regulation addresses general safety (including some digital aspects), the CRA provides the specific, detailed cybersecurity requirements. A cyber compromise could lead to a physical safety issue, linking the two regulations in practice.
- Retroactive Application: The reporting obligations apply to products already deployed in the field if they are still within their defined support period. Substantial modifications to existing products may also trigger new compliance requirements.

Q1: Software and Products with Digital Elements

Q: Please correct me - software (if networked and not isolated) is also PwDE? Hardware is not necessary?

A: Yes. A Product with Digital Elements (PwDE) can be software-only; hardware is not required. The CRA applies to hardware products, software products, and their associated remote data processing solutions. Therefore, standalone software can be in scope even if no physical device is involved, provided it is placed on the market and does not fall under an exclusion.

Q2: Scope of CRA Beyond Operating Systems and Antivirus

Q: Is it only operating systems, PKI software, or antivirus that fall under the CRA? Definitely not only embedded software?

A: Correct. The CRA is not limited to operating systems, PKI software, antivirus products, or embedded software. Those categories appear in Annex III and Annex IV because they are classified as Important or Critical products, but ordinary software

can also be a PwDE and therefore fall under the CRA. Examples may include desktop applications, mobile apps, device management software, monitoring platforms, field service applications, and other software products placed on the market.

Q3: Software Evaluation and Support Requirements

Q: Not only software mentioned in Annex III/IV? Do we need to evaluate and later support all software?

A: The key question is not whether software appears in Annex III or Annex IV, but whether it qualifies as a Product with Digital Elements. If software is a PwDE and placed on the EU market, it should be assessed for CRA applicability. If in scope, the manufacturer will need to comply with the relevant CRA obligations, including cybersecurity requirements, vulnerability handling, and support-period obligations. Annex III and IV mainly affect the conformity assessment route, not the basic applicability of the CRA.

Q4: CE Marking on Software

Q: How do you place a CE mark on software?

A: Software covered by EU product legislation can bear a CE marking even when distributed digitally. The practical implementation (e.g., within the installation package, installer, user interface, documentation, or accompanying materials) depends on the applicable legislation and conformity assessment route. The manufacturer must be able to demonstrate compliance and provide the required documentation and declaration of conformity. Specific implementation details continue to evolve through guidance and harmonized standards.

Q5: CE Marking Requirements for Software

Q: Is there any requirement in law or standards describing exactly how to place the CE mark on software?

A: The requirements stem from the applicable EU product legislation and general CE-marking rules. The CE marking must be visible, legible, and appropriately associated with the product. For software distributed digitally, manufacturers

commonly place the CE marking within the software, accompanying documentation, packaging, download portal, or installation materials. Additional guidance and harmonized standards are expected to provide further practical detail.

Q6: Remote Data Processing Solutions

Q: What exactly is considered a "Remote Data Processing Solution" in the context of the CRA?

A: A Remote Data Processing Solution is a remote or cloud-based functionality that is necessary for a product with digital elements to perform one or more of its intended functions. Examples may include cloud analytics platforms, device management portals, telemetry processing services, customer dashboards, or backend APIs that the product depends on. If the product relies on the remote service to provide its intended functionality, that service should generally be considered part of the product context for CRA purposes.

Q7: Machinery Regulation and CRA Relationship

Q: What is the relation between the Machinery Regulation (EU) 2023/1230 and the CRA?

A: The two regulations are complementary. The Machinery Regulation focuses on safety, including cybersecurity-related risks that may create hazardous situations. The CRA focuses on cybersecurity throughout the product lifecycle. Connected machinery can fall under both regulations simultaneously. In practice, manufacturers of connected machinery will often perform one integrated risk assessment covering both cybersecurity impacts and safety impacts resulting from cyber threats.

Q8: Monitoring Resources for Actively Exploited Vulnerabilities

Q: What kind of resources need to be monitored for actively exploited vulnerabilities? Is CISA KEV enough?

A: CISA KEV is a good source, but it is not sufficient on its own. Manufacturers should also monitor sources such as EUVD (European Vulnerability Database), CVE / NVD feeds, vendor security advisories, etc. along with vulnerability disclosures

received through CVD processes. The objective is to identify vulnerabilities affecting both the product and its dependencies/components.

Q9: Obligations for Products Already Deployed

Q: Do the September 2026 and December 2027 obligations also apply to products already deployed in the field?

A: Generally yes, but the answer depends on the specific obligation and product situation. Article 14 reporting obligations begin applying on 11 September 2026, while most other CRA obligations apply from 11 December 2027. Products placed on the market before those dates are not automatically re-certified. Applicability should therefore be evaluated based on the product lifecycle, support period, and specific CRA provisions rather than solely on the original placement date. A product inventory and support-period review is recommended.

Q10: Awareness of Incident and Reporting Timelines

Q: Does "aware of incident" mean receipt of an email, or validation of the report? When does the 24h/72h clock start?

A: The CRA requires reporting when the manufacturer becomes aware of an actively exploited vulnerability or severe incident. The regulation does not explicitly define awareness as the mere receipt of an unverified report. A practical and defensible approach is to document a formal validation and triage step. The reporting clock should start when sufficient evidence exists that the vulnerability or incident is valid, applicable to the product, and meets the reporting criteria. Manufacturers should maintain an auditable "Awareness Date/Time" field in their incident or vulnerability register.

Q11: 14-Day Deadline for Fixes

Q: Does the 14-day deadline mean a fix must be found within 14 days?

A: For actively exploited vulnerabilities, the requirement is to submit a notification that includes a mitigation within 72 hours after being aware of the exploitation. Then, a full report within 14 days.

Nemko Digital

Q12: Application to Newly Delivered Products

Q: This only applies to products newly delivered into the market, correct?

A: Not entirely. The CRA primarily regulates products placed on the EU market, but manufacturers should not assume that only newly delivered products are relevant. Existing products that remain supported, products undergoing substantial modification, and products affected by Article 14 reporting obligations may still require assessment. Applicability should therefore be evaluated based on the product lifecycle, support period, and specific CRA provisions rather than solely on the original placement date.

Q13: Minimum Support Period

Q: Any minimum support period, or is it completely up to the company?

A: The CRA does not allow manufacturers to choose an arbitrary support period. The support period must be determined based on the expected product lifetime and documented appropriately. In general, the CRA establishes a minimum expectation of five years, unless the expected use period of the product is shorter. Manufacturers must communicate the support period to users.

Conclusion and Next Steps

The CRA represents a significant shift in how cybersecurity is regulated in the EU, moving from voluntary best practices to mandatory, lifecycle-spanning obligations with strict reporting timelines and potential fines for non-compliance.

Key Takeaways:

1.Immediate Action Required: The September 11, 2026, deadline for incident reporting requires immediate attention to establish vulnerability disclosure policies and internal triage workflows.

2.Broad Scope: Organizations must evaluate not just their physical devices, but also accompanying software and essential cloud services.

Nemko Digital

3.Risk-Based Approach: A thorough cyber risk assessment is the essential first step to determine a product's classification and the required compliance efforts.

Potential Next Steps for Attendees:

- Assess product portfolios against the CRA definitions (Annex 3 and 4) to determine classification (Default, Important, Critical).
- Establish or refine a Coordinated Vulnerability Disclosure (CVD) policy ensuring anonymous reporting capabilities.
- Implement internal workflows for triaging vulnerabilities and meeting the 24-hour, 72-hour, and final reporting deadlines.
- Conduct foundational cyber risk assessments for all relevant products.
- Engage with compliance experts, such as Nemko Digital, for gap analyses and strategic roadmapping.

Special Offer: Call with our CRA Experts Now!

Don't wait for the next step.

As a special offer for webinar participants, we are providing an exclusive opportunity to discuss your specific CRA compliance challenges directly with our experts.

- Open to Webinar Participants
- Complete Application Form
- Share the topic you want to talk about

Ready to get started? Scan the QR code in the webinar materials or visit the link below to apply for your expert consultation:

Nemko Digital