Davis Wright Tremaine LLP

Osborne Clarke

Preparing for the EU Cyber Resilience Act: A Roadmap for U.S. Companies

Andrew M. Lewis
Counsel, DWT

Tobias Rothkegel
Partner, Osborne Clarke



Today’s Speakers



Andrew M. Lewis

Counsel, DWT

San Francisco, CA

andrewlewis@dwt.com



Tobias Rothkegel

Osborne Clarke

Germany / EU

tobias.rothkegel@osborneclarke.com

CRA Overview and Applicability

The Cyber Resilience Act is a binding EU law establishing broad, minimum cybersecurity requirements related to the design, development, and production of products with digital elements made available on the EU market.

EU Law: CRA is a regulation, not a directive and does not require individual member state adoption.

Product with Digital Elements: Software or hardware and their remote data-processing solutions. Broadly applies to nearly all hardware or software that can be connected to another device or network.

Made Available on the EU Market: Applies where covered products are supplied for distribution or use on the EU market in the course of a commercial activity (for free or charge).

Timeframe: Most obligations triggered in December 2027, but incident reporting began on September 11, 2026.

What is Different About CRA?

Broad, uniform level of cybersecurity across the European Union.

Product-focused: Applies to covered hardware and software products, including certain integrated remote data processing solutions. Not sector specific.

EU market trigger: Applies where covered products are supplied for distribution or use on the EU market in the course of a commercial activity.

Role-based obligations: Assigns obligations to manufacturers and responsibilities to importers, distributors, and authorized representatives.

Lifecycle obligations: Regulates cybersecurity from design and development through vulnerability handling, reporting, updates, and post-market action.

U.S. Company Applicability

Requirements apply to the manufacturer, importer, distributor, and authorized representatives.

Examples of qualifying activity:

- Direct sales or downloads into the EU.
- EU subsidiaries placing products on the market.
- EU importers or distributors demanding compliance evidence and contractual protections.
- OEM, embedded-component, white-label, and private-label relationships.

KEY POINT: For U.S. companies, the central question is whether a product reaches the EU market, not where the company is incorporated.



What Does CRA Require?

SECURE PRODUCT DESIGN

Design, develop, and produce covered products in accordance with essential cybersecurity requirements, including secure-by-default configurations.

CYBERSECURITY RISK ASSESSMENT

Document product cybersecurity risks and use the assessment throughout planning, design, development, production, delivery, and maintenance.

VULNERABILITY HANDLING

Identify, document, remediate, and disclose vulnerabilities; provide security updates throughout the support period.

INCIDENT + EXPLOITATION REPORTING

Report actively exploited vulnerabilities and severe incidents through the CRA reporting process within the applicable deadlines.

CONFORMITY + MARKET ACCESS

Prepare technical documentation, complete the applicable conformity assessment, issue the EU declaration of conformity, and affix CE marking.

POST-MARKET RESPONSIBILITY

Monitor products after launch, maintain contact channels, take corrective action, and cooperate with market-surveillance authorities.

Cybersecurity Risk Assessment

Documented assessment: Assess cybersecurity risks associated with the product and include the assessment in the technical documentation.

Lifecycle use: Take the assessment into account during planning, design, development, production, delivery, and maintenance.

Intended and foreseeable use: Evaluate relevant risks in light of the product's intended purpose and reasonably foreseeable use.

Updates when facts change: Revisit the assessment as product functionality, threats, vulnerabilities, dependencies, or intended use evolve.

Retention and evidence: Maintain the assessment and supporting technical documentation for the applicable regulatory period.

TIPS

The risk assessment drives many of the other requirements, including, among others, requirements to:

- Protect confidentiality, availability, and integrity of data
- Minimize processing of data
- Minimize negative impact of the products on other devices

Secure Product Design

Risk-based security: Design and develop the product to achieve an appropriate level of cybersecurity based on identified risks.

Secure by default: Make secure configurations the default and allow reset to the original state, subject to product-specific considerations.

Attack-surface reduction: Protect against unauthorized access and limit exposed interfaces, privileges, and unnecessary functionality.

Protection of data and functions: Safeguard confidentiality, integrity, availability, authenticity, and essential product functions.

Resilience and containment: Reduce the impact of incidents and support continued or recoverable operation.

TIPS

Translate Annex I outcomes into testable release criteria for each product and version.

Vulnerability Handling

Identify and document: Establish processes to identify and record vulnerabilities and product components, including through an SBOM in a commonly used, machine-readable format.

Receive and disclose: Provide a contact point and coordinated vulnerability disclosure policy for reporting and handling vulnerabilities.

Remediate without delay: Address vulnerabilities, including through security updates, and communicate relevant corrective information to users.

Distribute updates securely: Ensure security updates are disseminated securely and, where applicable, separately from functionality updates.

Support period: Handle vulnerabilities and provide security updates during the declared support period, generally reflecting expected product use and subject to statutory criteria.

TIPS

- Publish a monitored security contact and a coordinated vulnerability disclosure policy.
- Generate an SBOM and preserve the link between components, suppliers, products, and affected versions.
- Security updates must remain available for a minimum of 10 years or the remainder of the support period, whichever is longer.
- Security updates must be made free of charge (unless a tailor-made product).

Conformity and Market Access

Classify the product: Determine whether the product follows the default route or is an important or critical product under the CRA annexes.

Select the assessment route: Use the conformity procedure available for the product category, including third-party assessment where required.

Compile technical documentation: Document product design, risk assessment, development and production controls, testing, vulnerability handling, and other required evidence.

Declaration and CE marking: Issue the EU declaration of conformity and affix CE marking only after the applicable requirements are satisfied.

Preserve records: Retain required declarations, documentation, and conformity evidence and make them available to authorities.

TIPS

- Classify the product early and preserve the rationale, including the exact Annex III or IV category considered.
- Identify early where third-party review may be required.

Incident and Exploitation Reporting

Actively exploited vulnerability: Report when reliable evidence indicates that a malicious actor has exploited a vulnerability in the product.

Severe incident: Report incidents affecting product security that meet the CRA severity standard.

Early warning: Submit the initial notice within 24 hours after awareness, including available high-level information.

72-hour notification: Provide the available assessment, severity, impact, and corrective or mitigating measures.

Final report and user information: Complete the required follow-up report and inform affected users.

TIPS

- Maintain 24-hour and 72-hour templates that separate confirmed facts, assumptions, and open questions.
- Test single reporting platform.
- Consider CRA, NIS2, GDPR, DORA, and other laws simultaneously.

Post-Market Responsibility

Monitor the product: Collect and assess information about vulnerabilities, incidents, non-conformity, and cybersecurity risks after release.

Maintain contact channels: Keep vulnerability-reporting and authority contact mechanisms available and operational.

Corrective action: Bring non-compliant products into conformity and, when necessary, withdraw or recall them.

Inform and cooperate: Notify relevant economic operators and authorities where required and cooperate with market-surveillance requests.

Lifecycle Security Updates: Products must receive security updates for at least 5 years.

Control product changes: Evaluate whether modifications, new functionality, ownership changes, or rebranding affect conformity or shift manufacturer responsibility.

TIPS

- Track support periods, end dates, update commitments, and customer-facing lifecycle statements centrally.
- Reassess conformity before substantial modifications, rebranding, ownership changes, or major new functionality.
- Maintain an authority-response package with contacts, technical records, decisions, and distribution data.

Broader EU Framework

CRA

Products with digital elements

Manufacturers + supply chain

NIS2

Entity and network security

Essential / important entities

GDPR

Personal data breaches

Controllers + processors

DORA

Financial-sector operational resilience

Financial entities + ICT providers

AI ACT

AI system governance

Providers + deployers

Penalties and Enforcement Exposure

UP TO €15M

or 2.5% of worldwide annual turnover

Essential cybersecurity requirements; manufacturer obligations; incident and actively exploited vulnerability reporting.

UP TO €10M

or 2% of worldwide annual turnover

Specified obligations for authorized representatives, importers, distributors, declarations, CE marking, conformity assessment, and authority access.

UP TO €5M

or 1% of worldwide annual turnover

Incorrect, incomplete, or misleading information supplied to notified bodies or market-surveillance authorities.

HOW AUTHORITIES SET THE FINE

- Nature, gravity, duration, and consequences
- Prior similar fines against the economic operator
- Company size and market share, including SME/start-up status

FINES ARE NOT THE ONLY RISK

- Orders to bring a product into conformity
- Restrictions or prohibitions on EU market availability
- Product withdrawal or recall and cross-Member-State coordination

For U.S. companies, worldwide turnover and EU market-access remedies can make exposure materially larger than the fixed euro caps alone suggest.

Davis Wright Tremaine LLP

Questions? Reach out!



Andrew M. Lewis

Counsel, DWT

San Francisco, CA

andrewlewis@dwt.com



Tobias Rothkegel

Osborne Clarke

Germany / EU

tobias.rothkegel@osborneclarke.com