EXPLAINER

Cybersecurity Score – European Union (EU) Cyber Resilience Act

Cybersecurity Legislative Analysis Series

Bill Summary: Seeks to create conditions for the development of secure digital products and to improve cybersecurity awareness among digital product users.

Rating: CYBER CONCERNS Requirements in this bill have the potential to create unintended cyber consequences and/or allow threat actors to capitalize off of reported cybersecurity vulnerabilities. Legislation is undergoing "trilogue" negotiations toward a second reading by the European Parliament.

Status: European Union (EU) Cyber Resilience Act

Last updated: Oct. 23, 2023

Key Provisions

- Stipulates conditions for securely developing products with digital elements (e.g., connected devices, Internet of Things devices, mobile devices) and means to address vulnerabilities that arise throughout a product's lifecycle.
- Generates criteria that allow users to consider cybersecurity when selecting and using products with digital elements.
- Outlines specific areas for manufacturers and developers to improve cybersecurity and reduce the incidence of cyberattacks.
  - **Risk assessment:** Conduct risk assessments to address exploitable vulnerabilities, ensure secure-by-default configuration and limit attack surfaces
  - **Documentation:** Document product design, development and production; cybersecurity risk assessments; and declarations of conformity to EU standards
  - **Conformity assessment:** Conduct independent or self-assessments of conformance to the Act's requirements
  - **Vulnerability reporting:** Mandate reporting of cybersecurity incidents and vulnerabilities within 24 hours of discovery
- Provides affirmative defenses, including for platform core functionality concerns, complying with state and federal laws, and protecting user privacy and platform security.
- Specifies timeline to comply. (Failure to comply could result in fines or restrictions/prohibitions on product or service availability in the market.)
  - Mandates adherence to cybersecurity development standards within 40 months of the law's passage
  - Mandates timely security support and software updates to address vulnerabilities within one year after the law's passage

Background

The European Commission (the EU's executive body) proposed the Cyber Resilience Act (CRA) in September 2022 with the aim to formulate common cybersecurity standards for network-connected hardware and software products. This legislation is the EU's attempt to stymie the proliferation of cyber incidents affecting public and private entities across Europe by improving poor cybersecurity hygiene and development practices.

Cybersecurity Score – European Union (EU) Cyber Resilience Act

Cybersecurity Legislative Analysis Series

The CRA attempts to shift the burden of ensuring cybersecurity from end users to the companies that develop and manufacture software and hardware. Legislators argue that developers are best suited to mitigate and address cyber vulnerabilities and that it is easier to mitigate vulnerabilities as a developer than an end user. Similar concepts have been proposed by U.S. government entities, including the Cybersecurity and Infrastructure Security Agency's Secure by Design and Secure by Default principles and elements of the White House's National Cybersecurity Strategy.

The CRA aims to achieve four specific objectives to improve the cybersecurity posture of digital consumers, businesses and government entities:

- Ensure that manufacturers improve the security of products with digital elements in the design and development phase and throughout the whole lifecycle.
- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- Enhance the transparency of security properties of products with digital elements.
- Enable businesses and consumers to use products with digital elements securely.

Key Takeaways

The bill encompasses the entire lifecycle—from design to development to production—of essentially all network-connected devices and software. This expansive reach could significantly impact private industry's ability to innovate and may disproportionately burden any individuals, nonprofits or other entities that develop or support devices and software. While the CRA has the potential to improve Europe's cybersecurity posture, industry groups and concerned practitioners have criticized multiple aspects of the legislation including Software-as-a-Service exclusions, end-of-life software considerations, challenges associated with open-source software and guidance on software bills of materials, or SBOMs. This analysis is non-exhaustive, but is intended to provide an overview of cyber concerns, such as:

- **Vulnerability notification concerns:** Requiring companies to notify the European Union Agency for Cybersecurity (ENISA) of any cyber incidents and vulnerabilities within 24 hours of becoming aware of them—and take measures to resolve them—could disproportionately burden companies and allow threat actors to target these newly reported vulnerabilities for exploitation.
- **Compliance concerns:** Direct compliance costs for businesses (e.g., security requirements, information obligations, documentation, testing, reporting) are expected and will vary depending on their offerings. Similarly, there will be compliance costs for public authorities to conduct enforcement and information collection and dissemination.
- **Global implications:** Importers and distributors of technology products will have to verify their products' conformance to the bill's requirements, which could hamper technology rollout in Europe. Additionally, businesses will have to ensure compliance not only with the CRA, but with other countries' cybersecurity laws and regulations as well.

Free markets. Real solutions.

EXPLAINER

Cybersecurity Score – European Union (EU) Cyber Resilience Act

Cybersecurity Legislative Analysis Series

Cybersecurity Analysis

FACTORS	ANALYSIS
Access provisions	The CRA obligates companies to disclose cyber incidents and vulnerabilities within 24 hours of becoming aware of them (Article 11). It is unclear whether the data could be used by European intelligence or other government entities for other purposes. Enforcement authorities also have the power to request and access any internal documentation created or maintained under the CRA (Article 41). Additionally, they have the authority to access company data to assess the design, development, production and vulnerability handling of company products (Article 42).
Applicability	Given the ubiquity and usage of digital products, this bill would affect consumers and businesses globally. This may complicate or contradict business operations in global markets, especially with the United Kingdom and the United States. The EU is aware of the legislation's global ramifications and aspires to be the standard-bearer for software cybersecurity requirements.
Business impact	Companies would incur costs to alter their business operations to adhere to the bill's compliance and enforcement provisions (or if they are found to be in violation). The EU has estimated that aggregated compliance costs could be between 13 and 29 billion euros (EUR); end users may also end up paying higher prices. Failure to comply with requirements could result in EUR 15 million fines or up to 2.5 percent of total global turnover. Additional penalties are listed under Article 53.
Accounts for different entities	This bill has the potential to affect software and hardware developers of all sizes. Developer obligations under the CRA will differ depending on the classification of software (non-critical, critical class 1 and critical class 2, as detailed in Article 6 and expanded upon in Annex III).
Data privacy and security	The legislation views enhancements in end-user data privacy and data security as a positive side effect of cybersecurity regulation; however, it does not discuss how organizations would ensure data privacy and data security.
Rulemaking or update mechanisms	According to the draft text, each member state shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of the CRA (Article 41). Furthermore, a dedicated administrative cooperation group shall be established for the uniform application of the regulation (Article 41).
Exemptions, exceptions and defenses	Due to the freely distributed nature of open-source software, developers may not have a comprehensive understanding of all end users of their products (or which components would be monetized), which means that they could not feasibly comply with CRA requirements. After open-source communities raised concerns about open-source code being subject to the regulation, lawmakers adopted an amendment to the text exempting certain cases of open-source development from complying with the regulation; however, concerns remain regarding the use of open-source elements in for-profit endeavors.
Enforcement mechanisms	Member states designate surveillance authorities to ensure implementation.

Cybersecurity Score – European Union (EU) Cyber Resilience Act

Cybersecurity Legislative Analysis Series

Recommendations

We put forth the following recommendations with the goal of reducing some of the legislation's cyber impacts.

SUMMARY	RECOMMENDATION(S)
Compliance and certification timeline	**Policymakers should provide additional implementation context with a roadmap of required obligations as well as assessment, certification and compliance timelines and allow businesses to alter their development and manufacturing timelines accordingly.** Though amended legislation increased businesses' compliance timeline from 24 months to 40 months, companies may still face a bottleneck in addressing cybersecurity concerns depending on whether they can conduct independent assessments versus seeking out third-party assessments.
Reporting obligations	**Require reporting for significant cybersecurity incidents only (aligned with the EU's Security of Network and Information Systems (NIS2) Directive) rather than all cyber incidents in order to ease administrative burdens and limit the risk of threat actor exploitation.** **Do not mandate reporting of unpatchable vulnerabilities. Instead, ENISA could create a catalog of known exploited vulnerabilities or streamline information-sharing and patching initiatives.** Requiring companies to notify competent national authorities (originally ENISA but recently amended to "computer security incident response teams," or CSIRTs) of any cyber incidents and vulnerabilities within 24 hours of becoming aware of them and to take measures to resolve them could disproportionately burden companies and EU agencies while allowing threat actors to target newly reported vulnerabilities for exploitation. Notification of an active vulnerability within 24 hours, whether or not a patch or update is available, can introduce great risk.
Regulatory harmonization	**Ensure regular convening of relevant entities to consider harmonization efforts that avoid duplicity and contradiction and ensure consistency in terminology, timelines and compliance requirements.** The CRA is one of the most comprehensive bills to date that stipulates requirements for digital products; however, elements of the legislation overlap with others including EU's NIS2 Directive and parallel laws and regulatory guidance in the United States and other countries.
Definitions	**The European Commission should provide greater clarity on these concepts— including methodologies for determining categorization and ensuring regulatory consistency, as well as on obligations for developers and manufacturers—as they evolve.** Several areas of the CRA lack clarity, thus muddying the understanding of implementation and compliance guidelines. For example: • What type of software updates would be considered "substantial modification," thereby requiring a new conformity assessment (Article 3)? • What criteria must a product meet to be considered a "critical product" (Annex III)?
Capacity building	**Consider how workforce development will help fulfill the CRA's enforcement criteria.** Implementation and enforcement of such a comprehensive cybersecurity bill will require support from a workforce within the EU and EU member states as well as within research communities and industry, particularly small- and medium-sized enterprises.