datainnovation.org

Kir Nuthi, Senior Policy Analyst
knuthi@datainnovation.org

An Overview of the EU's Cyber Resilience Act

On September 15, 2022, the European Commission presented a draft law—the Cyber Resilience Act—to bolster the cybersecurity of digital products in the European Union and address existing cybersecurity regulatory gaps. The proposed regulation applies a broad horizontal regulatory framework to tangible and intangible products with digital elements—including connected devices and non-embedded software—to enforce cybersecurity standards on the entire digital supply chain.

What Does the Cyber Resilience Act Cover?

The Cyber Resilience Act applies to "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately." It will apply to these products throughout their entire lifecycle—from the design phase through to the obsolescence phase.

The Cyber Resilience Act covers tangible digital products, such as connected devices, and non-tangible digital products, such as software products embedded into connected devices. In essence, the Cyber Resilience Act seeks to cover digital products on the EU market that connect to the Internet and Internet-connected software.

What Are the Specific Objectives of the Cyber Resilience Act?

In 2020, global cybercrime cost €5.5 trillion, and global cybercrime will likely cost $10.5 trillion by 2025.[1]

To combat these growing cybersecurity costs and address vulnerabilities, the Commission notes four specific goals for the Cyber Resilience Act:

1. To ensure manufacturers improve the cybersecurity of covered products throughout the whole life cycle;
2. To create a single, coherent framework for cybersecurity compliance in the EU;
3. To increase the transparency of cybersecurity practices and properties of products and their manufacturers; and
4. To provide consumers and businesses with secure products ready for use.

It augments the EU's "Shaping Europe's Digital Future" strategy by bolstering the cybersecurity of Europe's data-driven economy. The Cyber Resilience Act mandates security-by-design by creating a list of essential cybersecurity requirements for manufacturers, importers, and distributors of connected devices and services to comply with through certification, reporting, and conformity assessments.

---

[1] Joint Research Centre, "Cybersecurity – Our Digital Anchor" (European Commission, 2020), https://publications.jrc.ec.europa.eu/repository/handle/JRC121051; Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" (Cybercrime Magazine, November 13, 2020) https://cybersecurityventures.com/cybercrime-damagecosts-10-trillion-by-2025/.

What Does the Cyber Resilience Act Specifically Exempt and Not Exempt?

The Cyber Resilience Act exempts connected devices that already have sectoral legislation, such as digital products regulated by the Medical Devices Regulation (Regulation (EU) 2017/745), In Vitro Diagnostic Medical Devices Regulation (Regulation (EU) 2017/746), Vehicle General Safety Regulation (Regulation (EU) 2019/2144), and Common Rules in Civil Aviation Regulation (Regulation (EU) 2018/1139).

The Cyber Resilience Act also does not apply to software-as-a-service unless the software-as-a-service is part of integral remote data processing solutions for a product with digital elements. The Cyber Resilience Act should only apply to free open-source software that is developed or supplied in the course of commercial activity. The recitals of the Cyber Resilience Act define commercial activity as charging for a product or technical support service, providing a software platform where the manufacturer monetizes other services, or using personal data for reasons that don't improve security, compatibility, or interoperability.

The Cyber Resilience Act also leaves open the possibility of further sectoral legislation post-enactment of the proposed text. Recital 14 describes how "sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential requirements laid down by this Regulation." In conjunction with how the Cyber Resilience Act's application can be limited if sectoral legislation achieves the same level of cybersecurity protection, this could lead to future changes in scope and interactions with the Cyber Resilience Act.

The Cyber Resilience Act does not exempt the European Digital Identity Wallets, electronic health record systems, or products with high-risk artificial intelligence systems.

How Does the Cyber Resilience Act Categorize Covered Products?

The Act splits covered products into three categories:

1. Class I
2. Class II
3. Unclassified or Default

The Default category applies to products without critical cybersecurity vulnerabilities. Companies responsible for these products will have to self-assess their vulnerabilities for improvement. According to the Commission, this category will cover 90 percent of connected devices, including photo-editing software, video games, and other commonplace software and devices.

The remaining products are split into Class I and Class II based on their level of risk. Risk factors for products include:

- Whether it runs with privilege, privileged access, or performs a function critical to trust
- Whether it is to be used in sensitive environments as described by NIS2
- Whether it is to be used to process personal information or other sensitive functions
- Whether its vulnerability can affect a plurality of people
- Whether it has already caused adverse effects when disrupted

Class I must adhere to the application of a standard or complete a third-party assessment to demonstrate conformity, while Class II must complete a third-party conformity assessment. Annex III of the Cyber Resilience Act currently splits critical products with digital elements into these categories. Still, these lists splitting Class I and Class II products can be expanded or reduced through later amendments to Annex III by the European Commission. The Commission is also empowered to adopt a delegated act supplementing the Cyber Resilience Act to specify the product category definitions in Class I and Class II lists.

What Are Class I Products in the Cyber Resilience Act?

Class I products have a lower cybersecurity risk level than Class II products but a higher level of risk than the unclassified or default category. A list of Class I products is found in Annex III of the bill and includes:

- Identity and access management software
- Browsers
- Password managers
- Malicious software detection
- Products that use virtual private networks
- Network management, configuration, monitoring, and resource management tools
- Security information and event management systems
- Update and patch management tools
- Mobile device and application management software
- Remote access software
- Physical network interfaces
- Microcontrollers
- Integrated circuits and gate arrays intended for use by essential entities described in the NIS2 directive
- Operating systems, firewalls, routers, modems, microprocessors, industrial automation and control systems, and industrial IoT that are not covered by Class II of the Cyber Resilience Act

It is important to note that it can be unclear which classification—Class I or Class II—specific products in product categories like operating systems that appear in both Classes will end up in. The European Commission will likely clarify these classification issues in subsequent delegated acts and amendments.

What Are Class II Products in the Cyber Resilience Act?

Class II are higher-risk products with digital elements with regard to critical cybersecurity vulnerabilities. They are also found in Annex III of the bill and currently include:

- Operating systems
- Hypervisors and container runtime systems
- Public key infrastructure and digital certificate issuers
- Firewalls for industrial use
- Industrial intrusion detection/prevention systems
- General purpose microprocessors
- Microprocessors for programmable logic controllers and secure elements
- Routers for industrial use
- Modems for industrial use
- Industrial switches
- Secure elements
- Hardware Security Modules
- Secure cryptoprocessors
- Smartcards, readers, and tokens
- Industrial Automation & Control Systems intended for the use by essential entities described in NIS2

- Industrial Internet of Things devices intended for the use by essential entities described in NIS2
- Robot sensing and actuator components and robot controllers
- Smart meters

How Is the Cyber Resilience Act Security-By-Design?

The Cyber Resilience Act requires companies to address information security and other cybersecurity vulnerabilities during the initial design and development of products—a process commonly referred to as security-by-design.

The Annexes to the proposed Act describe the various requirements for covered products, including what information companies should make available to users, conformity assessment procedures for higher-risk products, and technical documentation. But most importantly, Annex I delineates what the Commission deems "essential cybersecurity requirements" within the Cyber Resilience Act—"security requirements relating to the properties of products with digital elements." These include requirements using secure-by-default configurations and avoiding known exploitable vulnerabilities.

Annex I also details vulnerability handling requirements, defined as "essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle." These include requiring manufacturers to document vulnerabilities and components of a product as well as address and remediate vulnerabilities without delay. These vulnerability handling requirements ensure that products and related services must comply with the Cyber Resilience Act in every part of their life cycle.

What Are the Act's Essential Requirements for Connected Devices?

Manufacturers and developers must design, develop, and produce covered devices per the essential requirements in Annex I of the Cyber Resilience Act. Importers must only place products on the market that comply with the essential requirements in Annex I and that have manufacturers compliant with the essential vulnerability requirements. Distributors must also ensure that products with digital elements have a conformity marking and that the manufacturers and importers have complied with their necessary essential requirements obligations. In essence, these essential requirements create obligations for economic operators that design, develop, produce, and disseminate products with digital elements.

To show compliance, the manufacturers of these products must undertake a cybersecurity risk assessment, which they will then include in technical documentation and mark where certain essential requirements are not applicable. The manufacturers must then also update the product's risk assessment, have a process to report and remediate vulnerabilities, provide their EU declaration of conformity, and, if found unable to comply with the Cyber Resilience Act, inform market authorities that they will cease operations.

The Cyber Resilience Act splits essential requirements for connected devices into two major categories:

1. Security requirements relating to the properties of these products
2. Vulnerability handling requirements for the manufacturers of these products

What Are the Essential Security Requirements for Connected Devices?

To comply with the essential security requirements, connected devices and/or the manufacturers of connected devices must:

- Be designed, developed, and produced with an appropriate level of cybersecurity
- Be delivered without known exploitable vulnerabilities

- Be provided with a secure-by-default configuration
- Protect against unauthorized access through tools like authentication and identity management
- Protect the confidentiality of data by processing and potentially encrypting relevant data
- Protect the integrity of stored, transmitted, or processed data
- Minimize the collection of data to only process what is adequate and relevant for intended use
- Mitigate denial of essential functions or services
- Reduce the lack of availability of services provided by other devices
- Limit attack surfaces
- Reduce the exploitative effects and impact of a cybersecurity incident
- Record or monitor relevant security-related information
- Address future vulnerabilities through security updates, preferably automatic ones that notify users

What Are the Essential Vulnerability Requirements for IoT Manufacturers?

Manufacturers must do the following to comply with the essential vulnerability requirements:

- Document vulnerabilities and components of a product
- Address and remediate vulnerabilities without delay
- Have regular tests and reviews of their products' security
- Publicly disclose information about what vulnerabilities they fix
- Create and enforce coordinated vulnerability disclosure policies
- Facilitate information sharing about the vulnerabilities and provide a contact for said reporting
- Provide mechanisms to distribute updates that minimize exploitable vulnerabilities securely
- Disseminate security patches without delay and free of charge while providing users with a digestible explanation of what the patch is for

How Do the Cyber Resilience Act's Conformity Assessments Work?

For Unclassified or Default Category products, manufacturers will be responsible for determining and declaring their products satisfy all essential security and vulnerability requirements. These manufacturers will have to provide technical documentation, affix the conformity mark, and draw up a written EU declaration of conformity.

Manufacturers will have to undergo a third-party conformity assessment or apply harmonized standards or European cyber security certification schemes for Class I products. Class II product manufacturers can only demonstrate conformity through third-party conformity assessment. The specific requirements for third-party conformity assessments are described in Annex VI.

Do Manufacturers Have to Report Cybersecurity Incidents?

The Cyber Resilience Act creates reporting obligations for manufacturers to notify the European Union Agency for Cybersecurity (ENISA) within 24 hours after becoming aware of "any actively exploited vulnerability contained in the product with digital elements" or "any incident having impact on the security of the product with digital elements." The manufacturers will also inform the users of the product of the incident as well as corrective measures that can mitigate the consumer impact.

Similarly, importers and distributors of products with digital elements must inform manufacturers of cybersecurity vulnerabilities without delay. If there is a significant cybersecurity risk, importers and distributors must also inform national market surveillance authorities of the non-conformity and the corrective measures taken.

How Does the Cyber Resilience Act Interact With the Draft Artificial Intelligence Act?

The Cyber Resilience Act has particular provisions regarding high-risk artificial intelligence (AI) systems in Article 8 of the legislation. These provisions will only apply to high-risk AI systems defined by the draft AI Act.

Connected devices that fall within the scope of the Cyber Resilience Act and fulfill the security-by-design essential requirements will be considered in compliance with the draft AI Act and will be deemed to have the level of protection required by the declaration of conformity. For most of these products, the conformity assessment procedure of the AI Act applies, and it is up to regulatory bodies notified to control the conformity and notification procedures. Critical products, such as Class I and Class II products described by Annex III, will face the conformity assessment procedure of the Cyber Resilience Act on top of the AI Act requirements "in so far as the essential requirements of [the Cyber Resilience Act] are concerned."

Who Will Oversee the Act's Implementation and Enforcement?

National market surveillance authorities—chosen by the member states—will ensure the implementation of the Cyber Resilience Act. Each member state can choose one or more existing or new authorities to serve as the market surveillance authority. These institutions will cooperate with authorities designated under NIS2 or 2019's regulation on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification. The market surveillance authorities for the Cyber Resilience Act can coordinate with others from other member states, cooperate with ENISA, conduct sweeps to further enhance product cybersecurity, and report to the Commission annually. These authorities will have the power to impose administrative fines as laid down in the Cyber Resilience Act.

What Are the Penalties for Violations?

Non-compliance with Annex I's essential requirements and obligations in Articles 10 and 11 subjects offending businesses to the highest fine of either administrative fines of up to €15 million or 2.5 percent of their global annual turnover for the previous fiscal year, whichever is greater.

Non-compliance with other obligations within the Cyber Resilience Act will lead to administrative fines of up to €10 million or 2 percent of global annual turnover for the previous fiscal year, whichever is higher.

Misleading market surveillance authorities with incorrect, incomplete, or manipulated information will lead to a fine of €5 million or 1 percent of global annual turnover for the previous fiscal year, whichever is greater.

Member states can lay down effective, proportionate, and dissuasive rules on penalties applicable to businesses that fail to comply with the Cyber Resilience Act. Still, they must notify the Commission of the rules, measures, and subsequent amendments. National market surveillance authorities can also prohibit or restrict products from being available if the manufacturer, importer, distributor, or other responsible business proves non-compliant.

What Happens Next?

Now that the European Commission has presented the text, the Cyber Resilience Act will next make its way through the European Parliament. The European Parliament and the Council will examine, discuss, and propose amendments to the Cyber Resilience Act.

Once adopted, the regulation will be implemented in two phases. Within the first twelve months, manufacturers and developers of connected devices will be obligated to report exploited cybersecurity vulnerabilities and breaches. Within twenty-four months, member states and affected businesses will have two years to adapt to the new requirements proposed by the Cyber Resilience Act as it enters into force. After implementation, the Commission can re-review the regulation and create sectoral legislation for vulnerabilities that remain unaffected by the broad horizontal framework. Twelve months after the Cyber Resilience Act's entry into force, the Commission shall adopt its delegated act specifying the definitions of product categories in Class I and Class II that it was empowered to create in Article 6.

For Further Information

European Commission, "Cyber Resilience Act - Factsheet," September 15, 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020," September 15, 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

Freshfields Bruckhaus Deringer LLP, "Cybersecurity Resilience Act - EU proposes stricter cybersecurity rules for connected products," *Lexology,* September 15, 2022, https://www.lexology.com/library/detail.aspx?g=8307df51-bab1-4936-8c26-3ac9b5e99afd.

Kir Nuthi, "Feedback to the European Commission on the Cyber Resilience Act Initiative" (Center for Data Innovation, May 2022), https://www2.datainnovation.org/2022-cyber-resilience-act-roadmap.pdf.

ABOUT THE AUTHOR

Kir Nuthi is a senior policy analyst at the Center for Data Innovation focusing on European digital policy. Previously, she worked as a public affairs manager at NetChoice, where she focused on emerging technology issues surrounding content moderation, competition policy, and the sharing economy. Kir holds an MSc in International Public Policy from University College London and a BA with dual focuses in Economics and Political Science from the University of California San Diego.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, London, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the nonprofit, nonpartisan Information Technology and Innovation Foundation (ITIF).

contact: info@datainnovation.org

datainnovation.org