THHINKBV 2024

European Cyber Resilience Act (CRA)

The European Cyber Resilience Act is a legal framework that describes the cybersecurity requirements for hardware and software products with digital elements that are put on the market in the European Union. The Act has been introduced due to an increase in successful cyberattacks on hardware and software products. In 2021 it was estimated that the global annual cost of cybercrime was around €5.5 trillion. With the uptake of the act manufacturers are obliged to take security seriously throughout a product's life cycle.

Society and the economy are ever more reliant on digital solutions and so there is a need to protect against hacking of connected products and associated services. Experience shows that a cybersecurity incident in one product can affect an entire organisation or a whole supply chain. This can lead to severe disruption of economic and social activities and can even threaten the life of citizens. A problem is that vendors (hardware manufacturers, software developers, distributors and importers) often do not seriously consider cybersecurity, wanting to be first to market with a low-cost product. Adding cybersecurity requires qualified security engineers which has an impact on both product cost and in some cases performance, e.g. battery life. The response by companies to new vulnerabilities through a products' lifecycle is also often inadequate making it difficult for consumers to assess the security of the products and services they are using.

Current digital products are covered by several pieces of legislation, including EU legislation on specific products covering safety-related aspects and general legislation on product liability. However, this current legislation only covers some aspects related to cybersecurity of tangible digital products and associated embedded software. The General Product Safety Directive and the Machinery Directive do not prescribe specific cybersecurity requirements. In particular, the whole life cycle of a product or ancillary services and the need for regular software updates is not covered. The current legislation does not cover hardware that does not fall under the Radio Equipment Directive or the Medical Devices Regulation. As a result, the majority of hardware and software products are currently not covered by any cybersecurity legislation. In particular, the cybersecurity of non-embedded software is not covered by current legislation, which is a concern as it has become a main vector for cybersecurity attacks, causing significant societal and economic costs. Digital hardware and software products are a main avenue for successful cyberattacks and in a connected environment, a cybersecurity attack in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. Examples of this are:

- The Pegasus spyware, which exploited vulnerabilities in mobile phones.
- The WannaCry ransomware, which exploited a Windows vulnerability that affected computers across 150 countries.

- The Kaseya VSA supply chain attack, which used network administration software to attack over 1000 companies.

It was clear that although existing European legislation addressed certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain there was a need to set out mandatory requirements for the security of products with digital elements. At the European level, various programmatic and political documents, such as the EU's Cybersecurity Strategy for the Digital Decade, the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021, called for specific Union cybersecurity requirements for digital or connected products. This led to the creation of the Cyber Resilience Act.

The Cyber Resilience Act supersedes various acts and initiatives taken at Union and national levels which partially address identified cybersecurity related problems and risks. The aim is to provide increased legal certainty for both manufacturers and product users and avoid the unnecessary burden on companies to comply with a number of requirements in different countries for similar products. Products manufactured in one country are often used by organisations and consumers across the entire internal market. There are two major problems for users and the society:

- A low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
- An insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

This is further complicated by the fact that products with digital elements integrated in or connected to a larger electronic information system can serve as an attack site for malicious actors. As a result, even less critical hardware and software can be used to compromise a device or network, enabling malicious actors to gain privileged access to a system. The Cyber Resilience Act sets out two main objectives aimed to ensure the proper functioning of the internal market:

1. Create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
2. Create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Four specific objectives are set out:

1. Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle
2. Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers
3. Enhance the transparency of security properties of products with digital elements, and
4. Enable businesses and consumers to use products with digital elements securely.

Status

Political agreement between the European Parliament and Council on the Cyber Resilience Act was reached on 1st December 2023 and on 12 March 2024 the European Parliament approved the Cyber Resilience Act with 517 votes in favour, 12 against and 78 abstentions. See "European Parliament

legislative resolution of 12 March 2024 on the 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 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))". https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html In the next step it must be formally adopted by the Council.

Upon entry into force, manufacturers, importers and distributors of hardware and software products will have 36 months to adapt to the new requirements. A more limited 21-month grace period will be put in place for reporting obligations of incidents and vulnerabilities. The Council's common position is that there is a need for:

- Rules to rebalance responsibility for compliance towards manufacturers, who must ensure conformity with security requirements of products with digital elements that are made available on the EU market, including obligations like cybersecurity risk assessment, declaration of conformity, and cooperation with competent authorities.
- Essential requirements for the vulnerability handling processes for manufacturers to ensure the cybersecurity of digital products, and obligations for economic operators, such as importers or distributors, in relation to these processes.
- Measures to improve transparency on security of hardware and software products for consumers and business users, and a market surveillance framework to enforce these rules.

Examples of products with digital elements that come under the CRA

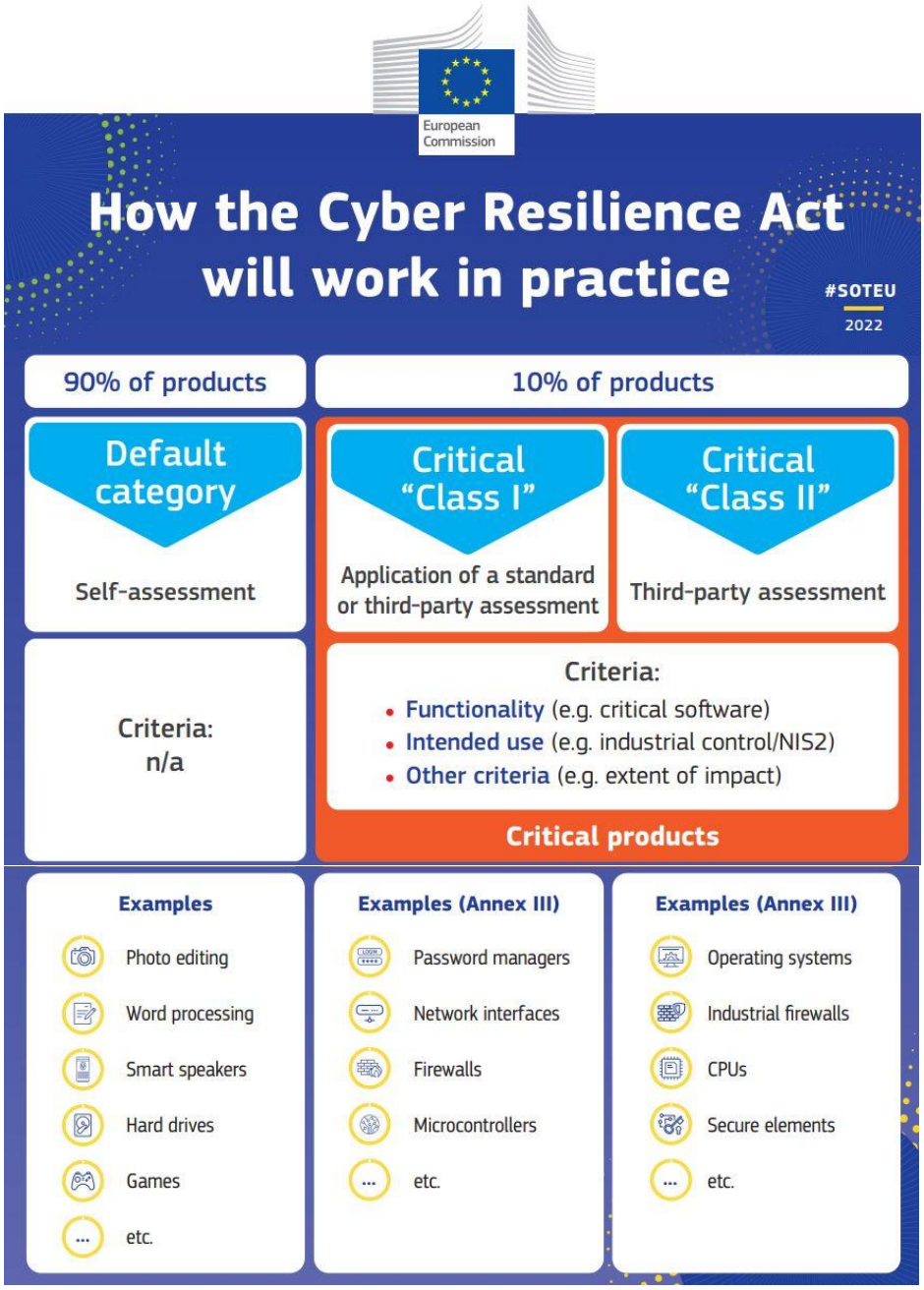
End Devices - Laptops, smartphones, sensors and cameras, smart robots, smart cards, smart meters, mobile devices, smart speakers, routers, switches, industrial control systems.

Software - Firmware, operating systems, mobile apps, desktop applications, video games.

Components (hardware and software) - Computer processing units, video cards, software libraries.

Thus, both products that can be connected physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces or any other types of software interface are covered by the act. As cybersecurity threats can propagate through various products with digital elements before reaching a certain target, for example by chaining together multiple vulnerability exploits, manufacturers should also ensure the cybersecurity of those products that are only indirectly connected to other devices or networks.

The CRA will thus have an impact on the entire software industry and addresses a broad range of products. There will be a big learning curve as companies transition to become compliant with the new legislation. A key aspect will be in proving conformity which requires assessment. In the majority of cases this can be done via self-assessment, however, Class I products will require adoption of a standard (which is currently being developed by CEN/CENELEC and ETSI) or via third party assessment and Class II products will require third party assessment.


European Commission
How the Cyber Resilience Act will work in practice
#SOTEU 2022
90% of products
10% of products
Default category
Self-assessment
Critical "Class I"
Application of a standard or third-party assessment
Critical "Class II"
Third-party assessment
Criteria:
n/a
Criteria:
• Functionality (e.g. critical software)
• Intended use (e.g. industrial control/NIS2)
• Other criteria (e.g. extent of impact)
Critical products
Examples
Photo editing
Word processing
Smart speakers
Hard drives
Games
etc.
Examples (Annex III)
Password managers
Network interfaces
Firewalls
Microcontrollers
etc.
Examples (Annex III)
Operating systems
Industrial firewalls
CPUs
Secure elements
etc.