MBB
MALTA BUSINESS BUREAU

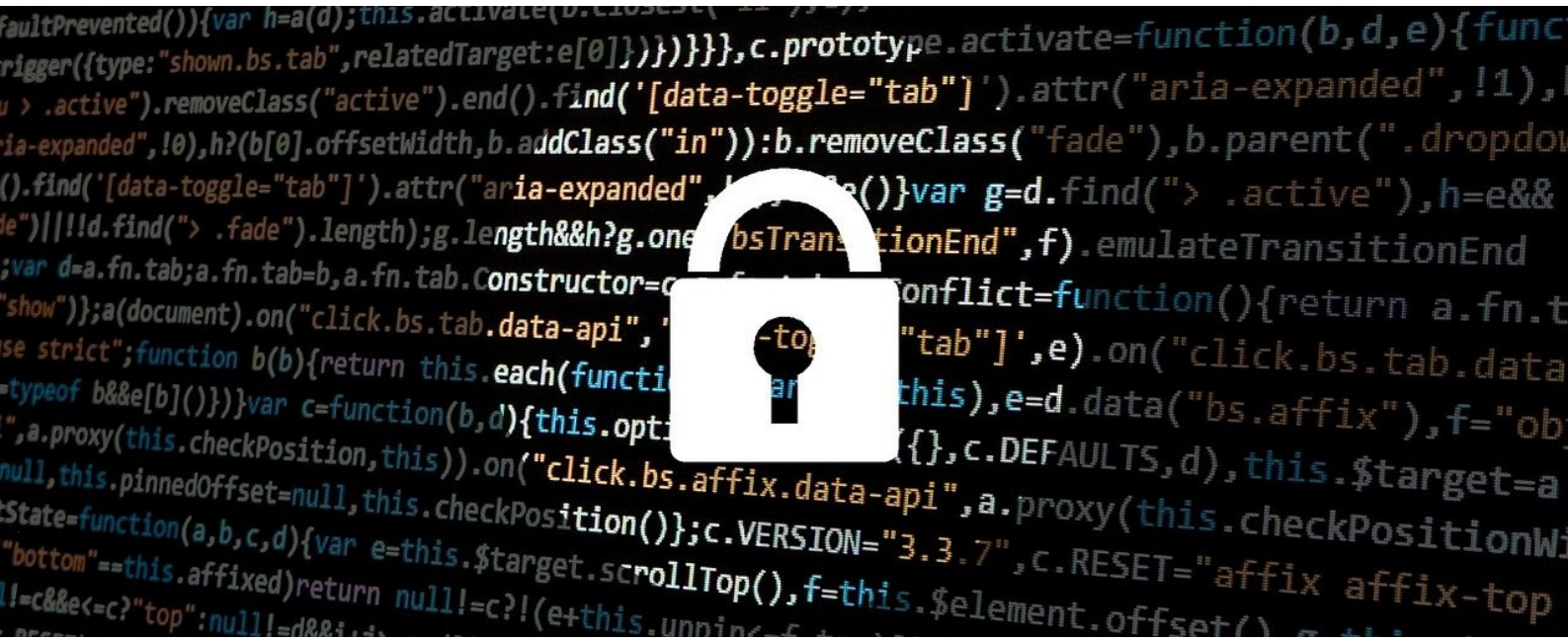
CYBER RESILIENCE ACT

POLICY BRIEF

DEC 2022

BACKGROUND

The Cyber Resilience Act (CRA) is the result of the EU's mission in becoming a leader in cybersecurity and will be complementing the existing frameworks of the Directive on the security of Network and Information Systems and the Cybersecurity Act. The need for yet more legislation on cybersecurity stemmed from the increasing number of high-profile cyberattacks which leave economic effects worldwide. The CRA framework will cater for tangible digital products – both wired and wireless as well as non-embedded software and will apply to their whole life cycle. A non-exhaustive list of examples of such products includes password managers, antiviruses, firewalls, routers and digital certificate issuers.



PURPOSE OF THIS ACT AND ITS MAIN ELEMENTS

The amount, complexity, scale, and impact of cybersecurity events have been increasing and as everything is connected, a cybersecurity incident can have widespread effects, disrupting many economic and social activities. In counteracting these risks, the Cyber Resilience Act introduces rules to protect digital products that are not covered by any previous regulation.

The CRA, in ensuring to contribute to the regular functioning of the internal market, has two main objectives:

(1) It aims to ensure that hardware and software products are available on the market are less susceptible to cyber threats and that manufacturers prioritise security throughout the product's lifecycle.

(2) It creates conditions which allow users to prioritise cybersecurity when purchasing or using products which incorporate digital elements

The objectives of the Cyber Resilience Act can be summarised as follows:

(a) To create an obligation to manufacturers to improve the security of products which incorporate digital elements throughout their whole life cycle;

(b) To create a comprehensive cybersecurity framework that allows hardware and software creators and manufacturers to be complaint with the new rules;

(c) To make the security properties of products with digital elements more transparent, and

(d) To enable businesses and consumers to securely use all products with digital elements.

THE CYBERSECURITY REQUIREMENTS FOR ORGANIZATIONS

The CRA will be introducing:

- Requirements for manufacturers during the designing, development and production phases to ensure an appropriate level of cybersecurity based on the risks;

- Requirements for manufacturers to deliver products that do not include any known exploitable vulnerabilities;

- Requirements in protecting the confidentiality and integrity of stored, transmitted or otherwise processed data;

- Obligation to only process data that is adequate, relevant and limited to what is necessary in relation to the intended use of the product;

- Obligation for developers to ensure that identified vulnerabilities are addressed through security updates complemented by notifications of available updates to users; and

- Compliance with specific rules for addressing vulnerabilities.

In expanding on the last point, manufacturers will need to be aware that as per the CRA framework, they will be obliged to report and identified vulnerabilities or incidents to the European Union Agency for Cybersecurity ("ENISA") within 24 hours of the manufacturer becoming aware of it. Manufacturers, will also need to notify users promptly and offer corrective measures to mitigate the impact of the vulnerability.

Obligations under the CRA will not be excusive to manufacturers but the framework will also apply to importers and distributors in the event they place a product on the market under their name or trademark, or substantially modify the product.

In the case of critical products with digital elements such as Internet browsers, antivirus software and operating systems, the CRA framework will subject these to stricter conformity procedures. Manufacturers of these critical products might also be obliged to obtain a European cybersecurity certificate under a European cybersecurity certification scheme.

Failure to comply with the Cyber Resilience Act may result in strict penalties as specified under Article 53 of the proposed CRA framework. Furthermore, member states also may establish supplementary penalties. In the meantime, Market Surveillance Authorities (and, in exceptional cases, the European Commission) may order non-compliant products to be brought into compliance, withdrawn from the market or recalled.

TIMELINE

If approved by the European Parliament and Council approve the framework in its current wording, organizations will have two years to adapt to the new requirements, with the exception of the rules regarding reporting of vulnerabilities and incidents, which will be effective one year after the Cyber Resilience Act enters into force.

The full text of the Commission proposal may be found here.

For questions or more detailed information please contact EU Affairs Manager Daniel Debono and Policy Executive Christine Said on infobrussels@mbb.org.mt