MBB
MALTA BUSINESS BUREAU

Cyber Resilience Act

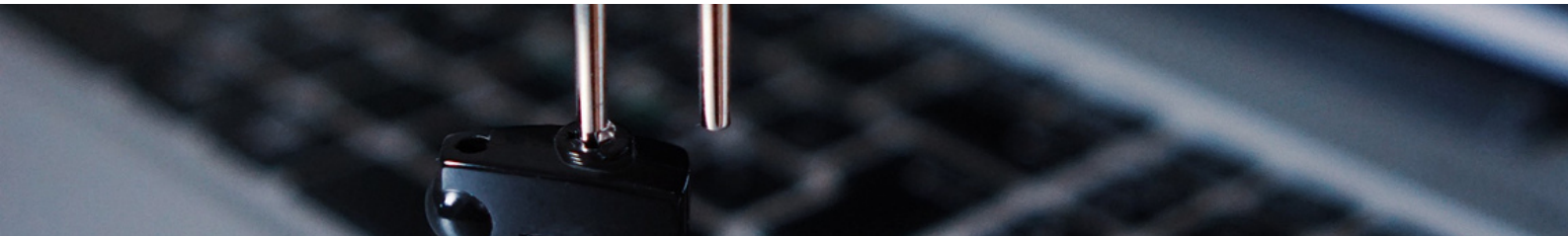
POSITION PAPER FEBRUARY 2023

BACKGROUND TO THIS PROPOSED LEGISLATIVE FILE

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.

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.



MARKET SURVEILLANCE

The current legislative proposal states that ''Member States may choose to designate any existing or new authority to act as market surveillance authority, including national competent authorities […] or designated national cybersecurity certification authorities.'' Aligning with the outcomes of consultations conducted by the European Commission, the EU needs to ensure that the wording in the final regulation takes into account the competences of each of the Member States. Local authorities need to have the necessary capacities and competences to consistently carry out successful checks and tests in ensuring conformity with the regulation before products reach the European market. Effective market surveillance is an essential component in ensuring the successful application of this legislation.

SECURITY BY DESIGN

In ensuring the effectivity of the CRA, the concept of security by design needs to be taken into consideration. In finalising this legislative framework, legislators need to work with industrial professionals in ensuring that European manufacturers apply the standards, techniques and methodologies to ensure that compliance with the CRA is ensured as much as possible from the very beginning of the lifecycle of a product. To achieve this, there needs to be harmonisation in terms of the methodology used and it needs to be communicated to European developers. This will help them in understanding what is to be developed, how and what needs to be done in achieving the secure development products and software. For example, app developers face extra costs in maintaining a cyber-resilient regiment for the benefit of consumers and it would be beneficial to them to have a set of guidelines or recommendations available in facilitating their compliance.

OPEN SOURCE SOFTWARE & COMMERCIAL ACTIVITY

The CRA appears to create an exclusion for open source software that is 'developed or supplied outside the course of a commercial activity', however the term commercial activity is not adequately defined and the brief explanation provided is ambiguous. Clarity must be provided in this regard, particularly since the development of the open source software can be independent of any later application, including application tied to commercial purposes.

OBLIGATIONS ON IMPORTERS & DISTRIBUTERS

The CRA obliges importers and distributors to refrain from placing a product with digital elements on the marks if the relevant operator 'considers or has reason to believe' that such product is not in conformity with the essential requirements set out in Annex I of the CRA. This obligation is additional to the obligations that importers and distributers have vis-à-vis confirming the fulfilment of specific criteria by manufacturers and also importers, in the case of distributors. In light of this, clarity is required as to what elements or factors would be relevant in this 'consideration' exercise that importers and distributors are meant to undertake.

HAVING REGULATORY SANDBOXES

The current wording of Article 24 does take into account the situation of SMEs given their limitations as it states that "notified bodies shall take into account the specific interests and needs of [SMEs] when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs." However, the final Regulation needs to be proportional in its scope. This can be ensured through the provision for the establishment of regulatory sandboxes in supporting SMEs and start-ups to comply with the provisions of this Regulation. For full context, a regulatory sandbox is a tool allowing businesses to explore and experiment with new and innovative products, services or businesses under a regulator's supervision. Taking the example of the Artificial Intelligence Act, clearly formulated wording and parameters within the final text needs to establish similar parameters for the creation and use of these regulatory sandboxes. This provision can work to the advantage of smaller companies and start-ups as it reduces their regulatory burden and ensure a higher degree of compliance. These regulatory sandbox cases can also provide insightful input into the needs of a future revision of the CRA.

HAVING A EUROPEAN CATALOGUE OF KNOWN VULNERABILITIES

The main aim of this Regulation is to increase the cybersecurity requirements of IoT devices. In doing so, manufacturers, importers and distributors are under the obligation of reporting identified vulnerabilities and instances of non-compliance to the relevant authorities. In keeping up with the EU's approach in having an EU-wide regulation, it would be of added value to also have further harmonisation among European developers and manufacturers by having access to a compiled list of the vulnerabilities identified by different member states. This also ensures further success and effectiveness of this regulation as well as ensures its complimentary with NIS2 Directive. The latter will among other measures streamline incident reporting obligations in avoiding over-reporting. Having an accessible catalogue will allow manufacturers to easily identify known vulnerabilities and flag these to the authorities within the timelines set by the NIS2 Directive.