EUROPEAN
COMMISSION

Brussels, 15.9.2022
SWD(2022) 283 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal of a Regulation for the European Parliament and of the Council

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Executive Summary Sheet (Max 2 pages)

Impact assessment on the Cyber Resilience Act (CRA)

A. Need for action

What is the problem and why is it a problem at EU level?

Hardware and software products often face successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. These products suffer from two major problems adding costs for users and the society: (1) a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and (2) an insufficient understanding and access to information by users, preventing them from choosing products with proper cybersecurity features or using them in a secure manner.

The cybersecurity of products with digital elements has a strong cross-border dimension, as products manufactured in one country are often used across the internal market. In addition, incidents initially affecting a single entity or a single Member State often spread within minutes across the entire internal market.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs. Recent examples are the Pegasus spyware, which exploited vulnerabilities in mobile phones, or the WannaCry ransomware worm, which exploited a Windows vulnerability, affecting computers worldwide.

What should be achieved?

Two main objectives were identified aiming 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 that manufactures 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 were set out**:** (i) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle; (ii) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software manufacturers; (iii) enhance the transparency of security properties of products with digital elements, and (iv) enable businesses and consumers to use products with digital elements securely.

What is the value added of action at the EU level (subsidiarity)?

The strong cross-border nature of cybersecurity and the growing incidents with spill-over effects across borders, sectors and products, mean that the objectives cannot effectively be achieved by Member States alone. Given the global nature of markets of products with digital elements, Member States face the same risks for the same product with digital elements on their territory. An emerging patchy framework of potentially diverging national rules also risks hampering an open and competitive single market for products with digital elements. Joint action at EU level is thus necessary to increase the level of trust among users and the attractiveness of products with digital elements place on the EU market. It would also benefit the internal market by providing legal certainty and achieving a level playing field for manufacturers of products with digital elements.

B. Solutions

What are the various options to achieve the objectives? Is there a preferred option or not? If not, why?

Four policy options and related sub-options were analysed going beyond the status quo: (1) soft law approach and voluntary measures; (2) product-specific ad-hoc regulatory intervention for cybersecurity of tangible products with digital elements and respective embedded software; (3) mixed approach, including horizontal mandatory rules for cybersecurity of tangible products with digital elements and respective embedded software and a staggered approach for non-embedded software, with two sub-options for conformity assessment; and (4) a horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of products with digital elements, including non-embedded software, with sub-options on the scope, and on conformity assessment.

The Impact Assessment concluded that the **preferred option** is option 4 covering all products with digital elements and foreseeing mandatory third-party assessment for critical products, based on the assessment of effectiveness against the specific objectives, efficiency of costs versus benefits, and conherence.

What are different stakeholders' views? Who supports which option?

When asked to rate the effectiveness of the policy interventions, the public consultation respondents agreed that option 4 would be the most effective measure (4.08 on a scale from 1 to 5). This includes consumer organisations (5.00), respondents identifying themselves as users (4.22), notified bodies (4.17), market surveillance authorities (5.00) and manufacturers of products with digital elements (3.85), including those of small and medium size (4.05).

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise of main ones)?

The preferred option would bring significant benefits to the various stakeholders. For businesses, it would prevent divergent security rules for products with digital elements and decrease compliance costs for related cybersecurity legislation. It would reduce the number of cyber incidents, incident handling costs and reputational damage. For the whole EU, it is estimated that the initiative could lead to a cost reduction from incidents affecting businesses by roughly EUR 180 to 290 billion annually. Furthermore, the initiative would lead to an increased turnover due to a growing uptake of products with digital elements. It would also improve the companies' global reputation leading to a demand uptake from outside the EU. For end users, the preferred option would enhance the transparency of the security properties and facilitate the use of products with digital elements. Consumers and citizens would also benefit from better protection of their fundamental rights, such as privacy and data protection.

What are the costs of the preferred option (if any, otherwise of main ones)?

The preferred option would add compliance and enforcement costs for businesses, notified bodies and public authorities, including notifying, accreditation and market surveillance authorities. For software developers and hardware manufacturers, it will increase the direct compliance costs for new cybersecurity requirements, conformity assessment, documentation and reporting obligations, leading to aggregated compliance costs amounting to up to roughly EUR 29 billion for an estimated market value of products with digital elements of up to EUR 1 485 billion in turnover. End users, including business end users, consumers and citizens may face higher prices of products with digital elements. However, these should be seen against the background of the significant benefits as described above. For notified bodies, the

additional costs are expected to be compensated by an increase in turnover.
What are the impacts on SMEs and competitiveness?
SMEs will be impacted by the new requirements both as manufacturers and end-users. In terms of compliance costs, SMEs would in principle be more affected than large companies which typically have better economies of scale and a greater cybersecurity awareness. However, SMEs would strongly benefit from the initiative, as cybersecurity embedded in products with digital elements would present a significant cost saving for SMEs as users. As manufacturers, SMEs would benefit from larger end-user trust and new customers. A seamless access to the internal market and a reduction of market fragmentation can be even more beneficial for SMEs, being less equipped to handle different regulatory requirements. While stressing the need for a proportionate approach and supporting measures, SMEs generally supported a level playing field between all companies and did not believe that they would be disadvantaged compared to larger companies in a scenario of horizontal mandatory requirements.
Will there be significant impacts on national budgets and administrations?
The initiative will impact national authorities, such as national notifying authorities, accreditation authorities and market surveillance authorities having responsibilities to monitor and enforce the proposed measures. These authorities will bear additional adjustment (e.g. training and human resources) and enforcement costs to take into account the new requirements. The resources spent by accreditation bodies are however offset and borne largely by conformity assessment bodies through the purchase of accreditation services.
Will there be other significant impacts?
No other significant negative impacts are expected. The preferred policy option would help reduce the number and severity of incidents, including personal data breaches and would have positive social impacts such as reducing cybercrime. The demand for security professionals is likely to grow and cybersecurity information asymmetries would be reduced.
Proportionality?
The preferred option does not go beyond what is necessary to meet the specific objectives satisfactorily. The intervention would ensure that products with digital elements are secured throughout their whole lifecycle and proportionally to the risks faced.
D. Follow up
When will the policy be reviewed?
By [36 months] after the date of application of the initiative and every four years thereafter, the Commission shall submit a report on the evaluation and review of the initiative to the European Parliament and to the Council.