Council of the European Union

Brussels, 16 September 2022
(OR. en)

12429/22
ADD 2

Interinstitutional File:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	15 September 2022
To:	General Secretariat of the Council
No. Cion doc.:	SWD(2022) 282 final - Part 1
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document 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

Delegations will find attached document SWD(2022) 282 final - Part 1.

Encl.: SWD(2022) 282 final - Part 1

EUROPEAN
COMMISSION

Brussels, 15.9.2022
SWD(2022) 282 final

PART 1/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

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) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 283 final}

TABLE OF CONTENTS

1. INTRODUCTION: EU POLITICAL AND LEGAL CONTEXT

In a more and more digitalised world, the number of high-profile cyberattacks keeps on increasing and the global annual cost of cybercrime was estimated to amount to EUR 5.5 trillion by 2021.[1]

Digital hardware and software products constitute one of the main avenues for successful cyberattacks. In a connected environment, a cybersecurity **incident 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**. This can lead to severe disruption of economic and social activities or even become life threatening. While the cybersecurity of providers of digital services is regulated at EU level under the Directive concerning measures for a high common level of security of network and information systems across the Union ('**NIS Directive'**),[2] the security of products with digital elements and in particular of software products is so far not subject to any comprehensive piece of EU regulation.

Products with digital elements (examples): *End devices, e.g.: 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 (both hardware as well as software): computer processing units; video cards; software libraries.*

There are numerous examples of noteworthy cyberattacks resulting from suboptimal product security, such as the **Pegasus** spyware, which exploits vulnerabilities in mobile phones and has been used by governments to spy on critics and opponents, as well as against prominent political leaders in Europe;[3] the **WannaCry** ransomware worm, which exploited a Windows vulnerability that affected 200 000 computers across 150 countries in 2017 and caused a damage amounting to billions of USD;[4] the **Kaseya VSA supply chain attack**, which used Kaseya's network administration software to attack over 1 000 companies and forcing a supermarket chain to close all its 500 shops across Sweden;[5] or the many incidents in which **banking applications are hacked** to steal money from unsuspecting consumers.

The **EU framework** comprises several pieces of horizontal legislation that cover certain aspects linked to cybersecurity from different angles (products, services, crisis management, and crimes), including measures to improve the security of the digital supply chain. In 2013, the Directive on attacks against information systems,[6] harmonising criminalisation and penalties for a number of offences directed against information systems came into force. In August 2016, the **NIS Directive** entered into force as the first piece of EU-wide legislation on cybersecurity. It introduced obligations on entities operating in key sectors of the European economies and societies, with a view to make them more resilient against cyber-attacks. More recently, the Commission proposed a review of this Directive ('NIS2 Directive proposal'),[7] which will most likely enter into force in 2022.[8] The upcoming NIS2 Directive raises the EU common level of ambition, through a wider scope, clearer rules, stronger supervision tools, a strengthened framework for operational capabilities and crises management and increased information sharing and cooperation. The new upcoming Directive also provides for **supply chain security**

[1] European Commission Joint Research Centre (2020): "Cybersecurity – Our Digital Anchor, a European perspective", page 7.
[2] Directive (EU) 2016/1148 (NIS Directive).
[3] For example: the Spanish Prime Minister: https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware.
[4] https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX.
[5] https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/.
[6] Directive 2013/40/EU.
[7] NIS2 proposal, COM(2020) 823 final.
[8] A provisional political agreement was reached in mid-May 2022.

obligations and related risk management measures. In 2019, the **EU Cybersecurity Act**[9] entered into force, aiming to enhance the security of ICT products, services and processes by introducing a voluntary certification mechanism.[10]

Cybersecurity of the entire ecosystem is ensured only if all its components are cyber-secure. The above-mentioned EU legislation has however substantial gaps in this regard, as it does not cover the security of products with digital elements (see gap analysis in *Annex 13*).

Improving the cybersecurity of key services through the NIS Directive will **not be enough to effectively improve cybersecurity throughout the supply chain**. Nor the voluntary cybersecurity certification schemes issued under the Cybersecurity Act where manufacturers do not have a legal obligation to certify their products would be enough to affectively address cybersecurity challenges.

The **current EU framework**[11] **applicable to products** that may also have digital elements comprises several pieces of legislation, including EU legislation on specific products covering safety-related aspects and general legislation on product liability. However, the current legislation covers only certain aspects linked to the cybersecurity of tangible products with digital elements and, where applicable, embedded software[12] concerning these products (e.g. Radio Equipment Directive – RED – and its relevant delegated act[13]). The EU regulatory framework on products (e.g. the General Product Safety Directive (GPSD) and the Machinery Directive (MD), both currently under review) does not prescribe comprehensive specific cybersecurity requirements.

These findings were also confirmed by an exploratory study contracted by the Commission and conducted in 2020-2021 to assess the need for horizontal cybersecurity requirements for products with digital elements, which also indicated that the benefits of the regulatory intervention would outweigh its potential costs.[14] A follow-up study[15] was also contracted by the Commission in early 2022, supporting this impact assessment.

While commonly accepted that an incident concerning products with digital elements can affect the whole system, it also appears more and more likely that the market will not be able to meet these constantly rising cybersecurity risks without an appropriate intervention from the policy makers.

At **global level**, security of supply chain and security of products with digital elements became prominent in recent years. Given that most products with digital elements are sold globally and not only within specific countries (for example, most organisations worldwide are using the same operating systems and a majority of smartphones across the globe is outfitted with the same types of microprocessor), the problems associated with the security of products with digital elements as described in the problem definition of this report are not specific to the EU but impact the rest of the world too. While cybersecurity product regulation is almost non-existing across the globe, several countries around the world have started to introduce measures (mainly voluntary) to address this issue. One of the most comprehensive sets of measures was taken by the Unites States of America as a result of significant supply chain attacks that affected the US administration. The measures focus on software and range from guidelines establishing best practices to detect vulnerabilities to requirements for critical software delivered to government

[9] Cybersecurity Act: Regulation (EU) 2019/881.
[10] The Cybersecurity Act allows the development of dedicated certification schemes. Each scheme establishes and lists the relevant standards. The decision to develop a cybersecurity certification is a risk-based one.
[11] Mainly New Legislative Framework (NLF) legislation. See for more details *Annex 11.*
[12] Software directly supportive to the function of the device on which the software is downloaded.
[13] C(2021) 7672 final supplementing RED, with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of the Radio Equipment Directive (RED).
[14] https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.
[15] Study by Wavestone, CEPS and ICF supporting the Commission preparatory work for the Cyber Resilience Act.

customers or a pilot program on cybersecurity labelling for Internet of Things (IoT) products. The UK is re-evaluating supply chain risks linked to ICT services and software and considering introducing soft law or regulatory measures. In Asia, various approaches are considered for supply chain security, such as a potential IoT security framework in Japan or cybersecurity labelling schemes of the likes of those recently introduced in Singapore. For more details on these global developments see *Annex 6.*

Noting the above-mentioned gaps in the EU legislative framework, various programmatic and political documents have called for **specific EU cybersecurity requirements for digital or connected products**.

The need for horizontal cybersecurity requirements for all products with digital elements on the internal market as the missing piece of the puzzle completing the picture of EU cybersecurity policies was not only identified in the context of development and implementation of recent EU cybersecurity legislation but also by relevant strategic and programmatic documents: The EU's Cybersecurity Strategy for the Digital Decade[16] of 16 December 2020 had already announced the establishment of common European cybersecurity standards for connected products. In her 2021 State of the Union address,[17] President von der Leyen announced a new European Cyber Resilience Act (CRA), planned for Q3/2022 under the Commission Work Programme 2022. Council Conclusions of 2 December 2020[18] and of 23 May 2022[19] have called for "*a horizontal regulation introducing cyber-security requirements"* covering "*the whole lifecycle of products with digital elements".* The European Parliament, in its Resolution of 10 June 2021,[20] welcomed *"the Commission's plans to propose horizontal legislation on cyber-security requirements for connected products and ancillary services".*

A horizontal intervention would put in place a framework for improving the security of products with digital elements. It would require manufacturers of hardware and software to take cybersecurity measures and improve transparency. This will reduce the number of vulnerabilities in such products and empower users to choose products matching their security needs and to use these products in a secure manner. It would aim to be one building block in the EU's endeavor to ensure a high level of cybersecurity throughout different supply chain levels, as well as in relation to its key concerned actors. At the same time, it would take a coherent and effective approach to preventing and countering cybercrime, all these ultimately for the benefit of consumers and citizens.

In the run-up to this impact assessment, the Commission has extensively consulted all relevant stakeholders. Member States, manufacturers, users, and other stakeholders were also invited to participate in the Open Public Consultation and in the surveys and workshops organised by the study supporting the Commission preparatory work for the upcoming regulatory intervention.[21] The Commission has also published a Call for Evidence, to which stakeholders could submit feedback. See also *Annex 2* on stakeholder consultation.

2. PROBLEM DEFINITION

2.1. What are the problems and what are their consequences?

Cybersecurity in products with digital elements is characterised by two major problems leading to a wide range of consequences and in particular to costs for users, both organisations and consumers, and society as a whole, mainly: (1) a **low level of cybersecurity of products with**

[16] JOIN(2020) 18 final.
[17] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701.
[18] See full text here.
[19] https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.
[20] 2021/2568(RSP).
[21] Study by Wavestone, CEPS and ICF supporting the Commission preparatory work for the Cyber Resilience Act.

digital elements, which is primarily reflected by the widespread prevalence of vulnerabilities and the insufficient and inconsistent provision of security updates, but also (2) an **insufficient understanding among users as regards the cybersecurity of products** because they are often not provided with the information necessary to choose products with appropriate cybersecurity features or to use products in a secure manner, leading to inadequately configured products.

The cybersecurity of products with digital elements has a particularly strong **cross-border dimension**, as products manufactured in one country (including third-countries), such as operating systems or laptops, are often used by organisations and consumers across the entire internal market. In addition, given the borderless nature of the Internet, incidents initially affecting only a single entity or a single Member State often spread within minutes across the entire internal market.

The widespread presence of vulnerabilities in products with digital elements used by organisations, such as critical infrastructure, or by consumers, as well as misconfigured products due to the users' inadequate choice of security settings,[22] have far-reaching consequences. Businesses and other organisations bear significant cost associated with mitigating the risks related to cybersecurity. In addition, they must respond to and recover from cyberattacks, which often propagate across national borders and throughout the internal market. There is also a cost to society when digital solutions are not taken up for fear of security risks. Finally, there is a risk that Member States may start to regulate products security at national level, leading to internal market fragmentation.

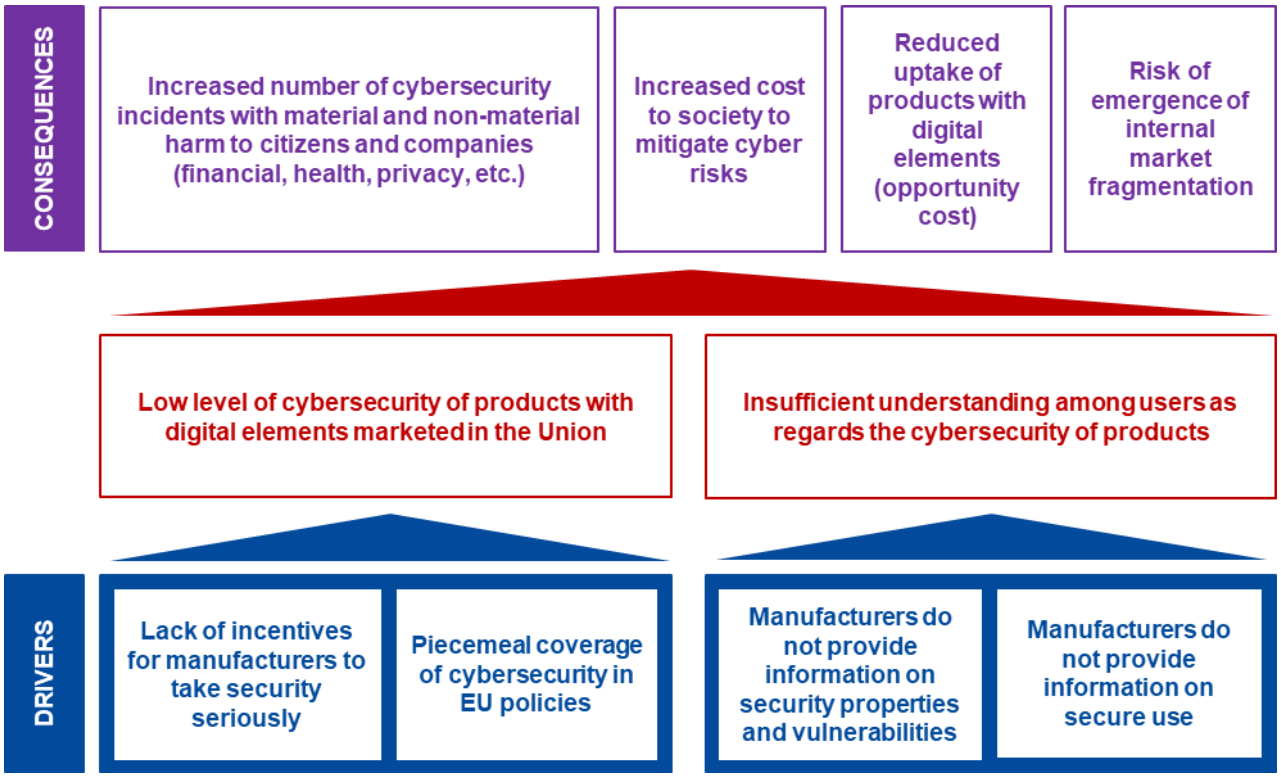

Figure 1: Problem definition

While fewer vulnerabilities in products with digital elements and more transparency on the side of manufacturers as regards the security properties and secure use of products would not eliminate such costs altogether, more secure hardware and software and better documentation and instructions could lead to a notable reduction in costs. Given that most attacks rely on vulnerability exploits, there would be fewer incidents to manage and recover from. If incidents

[22] From a cybersecurity perspective, a product with digital elements is misconfigured if the security settings chosen by the user do not adequately reflect the user's security requirements, leading to an increased attack surface and a higher risk of incidents.

became less likely, a number of risk mitigation measures, such as cybersecurity insurance, could become less expensive.[23]

2.1.1. Problem 1: Low level of cybersecurity of products with digital elements marketed in the Union

The vast majority of attacks on critical infrastructure or other essential services are the result of vulnerabilities in products with digital elements. The Commission's proposal for a revision of the NIS Directive requires companies to integrate supply chain security measures into their risk management processes. However, the security of such entities also depends a lot on the availability of secure products. Even the most diligent risk management process cannot offer a high level of organisational security if the market for products with digital elements does not cater to the security needs of organisations.

While a number of factors, such as badly configured systems and credential theft (e.g. through phishing), can facilitate or enable cyberattacks, the main attack vector for security breaches is the **exploitation of vulnerabilities in hardware and software**. Estimates of the share of incidents resulting from exploits against weaknesses in the computational logic and design of software range from 62 %[24] for operators of essential services identified under the NIS Directive to 90 %.[25] A large majority of vulnerabilities are exploitable over the Internet and do not require physical access to networks,[26] which explains why malicious actors are carrying out their attacks on European organisations from anywhere in the world.

Cyberattacks against individuals or organisations exploit vulnerabilities in software and hardware products deployed within the victim's network. To achieve their mission, malicious actors usually exploit multiple vulnerabilities at various stages of an attack[27] .[28] Preventing vulnerabilities during product development and identifying and closing vulnerabilities in products before they can be exploited could bring cyberattacks to halt at various stages of their development. For example, attackers might first exploit a vulnerability allowing them to breach the server hosting a company's website before making their way through the company's network to more crucial systems, such as key workstations and the sensitive data stored thereon.

The number of vulnerabilities recorded in vulnerability databases is increasing year-on-year. For example, vulnerabilities recorded under the US Common Vulnerabilities and Exposures (CVE) system have increased from 18 325 in 2020 to 20 150 in 2021. This is also valid for the high-profile vulnerabilities that are exploited by malicious actors and for which manufacturers have to date not provided any patch ("zero-days"). According to cybersecurity researchers and databases tracking vulnerabilities, to date the year 2021 has seen the so-far highest number of zero-day vulnerabilities in products with digital elements actively exploited.[29] As a result, the attack surface that malicious actors can exploit increased significantly. At the same time, the threat

---

[23] Insurers gather information about hardware and software vulnerabilities to improve their risk models and calculate risk premiums. See https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf, p. 10.

[24] Calculation based on the preliminary results of a still ongoing survey commissioned by ENISA and executed by Gartner (2022): NIS Investments Study 2022.

[25] Hao Wang and Andy Wang (2009): Security metrics for software systems, ACM-SE 47: Proceedings of the 47th Annual Southeast Regional Conference, p. 1.

[26] Gueye and Mell (2021): "A Historical and Statistical Study of the Software Vulnerability Landscape", *The Seventh International Conference on Advances and Trends in Software Engineering SOFTENG 2021*, p. 1.

[27] During the *initial reconnaissance* stage, attackers search for weaknesses in the victim's systems, including vulnerabilities in hardware and software. Exploiting vulnerabilities not only facilitates the *initial compromise* of a victim's systems but also allows an attacker to gain full control of a system and *move* to other systems within an organisation or network.

[28] For a snapshot of the distribution of recorded vulnerabilities across the various stages and techniques of an attack see Ampel, Samtani, Ullman and Chen (2021): "Linking Common Vulnerabilities and Exposures to the MITRE ATT&CK Framework: A Self-Distillation Approach", *2021 ACM Conference Knowledge Discovery and Data Mining*.

[29] For example, as of September 2021, the Zero-day tracking project had recorded 66 zero-days in use, as compared with just 37 in 2020. Source: https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/

landscape has evolved, with the number of documented major state-sponsored cybercrime groups[30] increasing year-on-year.[31]

While there is no universally applicable measurement of the aggregate level of security of products with digital elements marketed in the Union, a number of observations indicate that the **security of products with digital elements is low across the board**.

Vulnerabilities are regularly identified in all types of products, both hardware and software. When it comes to hardware, vulnerabilities are discovered both in integrated products sold in the market (such as smartphones, laptops or smart household appliances) as well as in hardware components, such as in memory, central processing units (CPUs) and other chipsets. Similarly, software vulnerabilities are found in all types of products, ranging from operating systems to user applications and even those products actually designed to help prevent incidents, such as anti-virus software.[32] Again, vulnerabilities are not only found in final products but also in intermediate software components, such as libraries, and including in open-source components. The Apache Log4j logging utility is the most recent example of a major vulnerability in a widely used open-source software component that has affected entities across the entire internal market. Log4j has been used by a wide range of major software manufacturers and the vulnerability, which has existed since 2013 but was only discovered in 2021, has led to security incidents across the globe.[33]

Moreover, the number of vulnerable devices connected to the Internet is increasing. For example, manufacturers are connecting more and more ICSs to the Internet. Between 2017 and 2018, the number of ICSs increased by 27 %.[34] According to a 2021 study, many companies are connecting operational technology (OT) directly to the Internet. Almost all devices analysed by the study contain at least one vulnerability, with Europe and North America being the most affected.[35]

Security is not only a concern in products deployed in an industrial or organisational setting, but also when it comes to consumer devices. A recent Euroconsumers probe into connected home devices, such as alarm systems and food processors, has revealed that two-thirds of devices contain vulnerabilities considered as 'of high severity' or 'critical', affecting both low-cost devices of unknown brands as well as products developed by well-known manufacturers.[36] Vulnerabilities in connected products are not only a theoretical concern, but their exploitation has a very real impact on consumers. For example, in 2019 cybercriminals breached Ring Home Security Cameras to observe citizens in their private homes and to speak with a small child in the child's room.[37]

Manufacturers of products with digital elements do not only place vulnerable products on the market, but they often also do little to improve security throughout the **life cycle** of their products. For example, a 2018 survey of smartphone manufacturers revealed that 14 out of 19 device manufacturers provide security updates for less than three years.[38] In addition, when manufacturers do provide updates fixing vulnerabilities, they often take too long. Even security flaws discovered by Google's Project Zero, which pressures manufacturers of browsers and other

[30] So-called advanced persistent threats (APT).
[31] See article here.
[32] https://thehackernews.com/2020/10/antivirus-software-vulnerabilities.html
[33] https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html
[34] https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019.
[35] Simon Daniel Duque Anton, Daniel Fraunholz, Daniel Krohmer, Daniel Reti, Daniel Schneider, and Hans Dieter Schotten (2021): "The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World", *IEEE Internet of Things Journal*, Volume: 8, Issue: 24, Dec.15, 15 2021.
[36] Euroconsumers (2021) *"Hackable home project: Euroconsumers unveils worrying results for smart device owners"*
[37] BBC (2019) https://www.bbc.com/news/technology-50760103.
[38] SecurityLab (2018), see the table here.

software into swiftly fixing vulnerabilities by threatening to disclose them after 90 days, are on average only fixed after 52 days.[39]

Finally, many manufactures do not even provide for means to contact them to report discovered vulnerabilities. Weaknesses in products with digital elements are not only discovered by the manufacturer of a product or a malicious actor, but also by other manufacturers,[40] security researchers, ethical hackers and even customers. Ideally, organisations should therefore develop their own vulnerability disclosure policies to facilitate interaction with these actors.[41] At the very least, organisations should provide for a means to report vulnerabilities to them.[42] According to the European Telecommunications Standards Institute, *"As of early 2022 only about only about 20 % of ICT and IoT companies have a publicly identifiable dedicated means to notify a company of a potentially serious security issue with their products or services."*[43]

The problems associated with non-secure products are exacerbated by the fact that in a range of markets for products with digital elements, the number of available products is very limited, creating a *monoculture*. As a result, whenever a new vulnerability is exploited, a relatively large number of users is affected at the same time. This monoculture is explained by the fact that in some instances the utility of products with digital elements, in particular software, increases with the number of people that use it. The importance of such *network effects* that dissuade users from diversifying the products that they use and their impact on cybersecurity have been long recognised.[44]

In addition, exploiting known vulnerabilities has never been easier and does often not require a particularly high degree of familiarity with the underlying weaknesses in the computational logic of targeted systems.[45]

Asked to rate the overall level of security of products with digital elements in the Union, the respondents to the Commission's public consultation on the initiative gave on average a 2.82 (on a scale from 1 to 5 with 5 indicating a very high level of cybersecurity)products with digital elements. The responses of the different stakeholder groups were as follows: national market surveillance bodies (1.5), consumer associations (1.7), public administrations as users (2.5), SMEs as users (2.5), hardware manufacturers (3.2), software manufacturers (2.8), SMEs in their role as manufacturers (3.2). In addition, an overwhelming majority of 95 % of respondents said that the level of risk of cybersecurity incidents affecting products with digital elements has increased during the last five years.

2.1.2. Problem 2: Insufficient understanding among users as regards the cybersecurity of products

While it is crucial to make products with digital elements more secure, cybersecurity incidents are in many cases also the result of users choosing products ill-fitted for their purposes or wrongly configuring hardware and software, thereby unnecessarily increasing the security risk of their device or network. This is the result of a number of factors, including a lack of

[39] Google Project Zero (2022).
[40] Some companies employ security analysts tasked with discovering vulnerabilities in products with digital elements of other manufacturers, such as for example Google's Project Zero, which reports vulnerabilities to manufacturers first and publishes them after a 90 day period.
[41] For example, by implementing EN ISO/IEC 29147, which provides requirements and recommendations to manufacturers on the disclosure of vulnerabilities in products and services.
[42] A popular standard is security.txt, a plaintext document that is placed on a manufacturer's website and which contains contact information for reporting vulnerabilities in a secure manner.
[43] See ETSI press release on the coordinated vulnerability disclosure report
[44] For an extensive discussion of the phenomenon, see Geer, Schneider et al (2003): "CyberInsecurity: The Cost of Monopoly", Computer & Communications Industry Association Report.
[45] Popular frameworks used by security analysists as well as by malicious actors contain thousands of vulnerability exploits that can be used out of the box to breach unpatched systems. For example, the Metasploit Framework, a popular penetration testing suite, contains almost 600 exploit modules to target systems running Linux, the most widely-used operating system for servers, as well as more than 1300 exploit modules that could be used to breach into Microsoft Windows installations.

cybersecurity awareness and skills of users, and a lack of information provided by manufacturers on security properties, vulnerabilities and secure use. For example, a study of a Dutch consumer protection organisation covering 86 manufacturers across 18 different product groups has revealed that only 1 out of 5 manufacturers provides information to customers about available security updates.[46]

Nothing is more revealing of the lack of understanding amongst users than the notorious neglect of urgent security updates. A survey from 2014 interviewing Microsoft Windows users suggested a lack of awareness and knowledge by users as well as a lack of clear information provided by manufacturers to users.[47] According to 2020 Eurostat data, around 48 % of EU citizens have never restricted or refused access to personal data, when using or installing an app on a smartphone.[48]

Asked in the consultations held by the study supporting this impact assessment to which extent an insufficient understanding of users of the security of products with digital elements has a negative impact on the security of individuals or organisations, 69 % of participants replied that the impact was at least moderate. Asked to rate consumers' awareness and understanding of cybersecurity properties of products with digital elements, consumer organisations gave an average rating of 2.33 (on a scale from 1 to 5). Asked in the public consultation to rate their own awareness of the cybersecurity risks associated with products with digital elements, consumer organisations gave a rating of 2.3 on behalf of consumers. Similarly, when asked to rate their understanding of the cybersecurity properties of products with digital elements and the skills to operate them securely, consumer organisations provided a rating of 1.7.

2.2. What are the problem drivers?

2.2.1. Driver 1: Lack of incentives for manufacturers to take security seriously

Manufacturers often neglect the security of their products. Almost 50 % of manufacturers knowingly place products with digital elements on the marked that contain vulnerabilities.[49] One of the main reasons for this is that manufacturers lack the necessary incentives to invest in a secure development life cycle (SDLC). This is the result of strong negative externalities in markets for products with digital elements, information asymmetries between manufacturers and users, a faced-paced market and the costs associated with secure development.

A recent international survey amongst almost 100 software development professionals of mobile health applications has revealed that *"little or no budget for employing security"* is considered the main challenge when it comes to application security, followed by *"insufficient security knowledge [amongst developers]"*. Other important challenges that were identified highlight deficiencies in the development life cycles of manufacturers, such as a *"lack of involvement of security experts"*, *"poor security decisions during development process"* and a *"lack of security testing"*.[50]

Asked in the public consultation whether manufacturers of software were effectively addressing cybersecurity vulnerabilities and incidents affecting their customers, the respondents gave an overall rating of 2.96 (on a scale from 1 to 5),[51] with consumer organisations rating the effectiveness of manufacturers very low (1.33). The responses of the other stakeholder groups were as follows: national market surveillance bodies (2.0), public administrations as users (2.8),

[46] https://www.consumentenbond.nl/nieuws/2022/fabrikanten-informeren-onvoldoende-over-updates

[47] K. E. Vaniea, E. Rader, and R. Wash (2014): "Betrayed by updates: How negative experiences affect future security", *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*.

[48] https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_SP20/default/bar?lang=en&category=isoc.isoc_i.isoc_ci_sci

[49] Security (2020): "Survey reveals nearly 50% of organizations knowingly push vulnerable software".

[50] Aljedaani, Ahmad, Zahedi and Babar (2020): "An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective", *2020 27th Asia-Pacific Software Engineering Conference (APSEC)*, p. 5.

[51] Respondents identified as users gave a rating of 2.66, while software manufacturers rated their measures with 3.43. Small and medium sized manufacturers provided a slightly higher rating of 3.53.

SMEs as users (2.3), hardware manufacturers (3.7), software manufacturers (3.4), SMEs in their role as manufacturers (3.5).

Users bear the costs associated with incidents and the market has negative externalities

While manufacturers of products with digital elements can sometimes face reputational damage when their products are found to be lacking security, the cost of vulnerabilities is predominantly borne by the users, such as operators of essential services, but also consumers. Examples of costs borne by users are risk mitigation costs, such as taking out cybersecurity insurance[52] or putting in place a security operation centre, as well as the costs resulting from a cybersecurity incident, such as the cost involved in recovering lost data. This limits the incentives of manufacturers to invest into secure design and development and to provide security updates.[53]

While it might seem intuitive to assume that manufacturers have an incentive to make their products secure and avoid the fallout of incidents involving their products, in reality it is rarely the companies affected by major cybersecurity incidents that suffer significant negative long-term consequences, but rather the users or customers.[54] One of the reasons why reputational damage often does not translate into users actually switching products consists of the high switching costs associated with replacing a product by another one: products are often heavily tied into existing operations. Moreover, in many cases products markets do not provide for a wide range of alternative products with digital elements. For example, there are only very few widely used operating systems for desktop computers and smartphones. Similarly, the chipset market is highly concentrated with only few companies offering desktop CPUs, video card chipsets and other components.

Respondents to the public consultation have identified costs borne by users as an important driver for the low level of security of products with digital elements: Respondents rated the *"The user bears additional cost when affected by a cybersecurity incident"* with 4.13 (on a scale from 1 to 5). The responses of the different stakeholder groups were as follows: national market surveillance bodies (4.7), consumer associations (5.0), public administrations as users (4.6), SMEs as users (4.6), hardware manufacturers (3.4), software manufacturers (3.9), SMEs in their role as manufacturers (3.6).

In addition, it is often not even the manufacturers or the users bearing the costs of incidents but unrelated third parties, such as the victims of DDoS attacks carried out using infected devices: Given the structural and persistent nature of such negative externalities in the markets for products with digital elements, a recent study on IoT device security has concluded that "The costs of security failures are often borne by other stakeholders than the owners of the device or the manufacturers. So, there is a market failure here that justifies government intervention."[55]

Information asymmetries

While the manufacturers of products with digital elements are normally not bearing the cost associated with vulnerabilities, they would have to bear the additional cost of making their products more secure. This raises the question if there could be any other incentives leading to an adequate level of investment in product security, such as competitive advantage derived from placing products with a high level of security on the market.

---

[52] The cost of cyber insurance is estimated to range from USD 650 to USD 2 357 for liability limits of USD 1 000 000 (i.e. EUR 950 0000) for companies with moderate risks: https://advisorsmith.com/business-insurance/cyber-liability-insurance/cost/.

[53] See Asghari, van Eeten and Bauer: "Economics of cybersecurity", in: Bauer and Latzer (2016): "Handbook on the Economics of the Internet", p. 267.

[54] Morgner and Benenson (2018): "Exploring Security Economics in IoT Standardization Efforts", *Workshop on Decentralized IoT Security and Standards (DISS) 2018*, p. 3.

[55] Rodríguez et al (2021): "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, for a more detailed discussion of IoT consumer device security, p. 13.

However, users are often unaware of the security risks associated with products with digital elements. While they may attribute value to secure products, they do not have the knowledge to understand the value stemming from a product that has been developed with security considerations mind. In addition, given the complexity of products with digital elements and the fact that users usually do not have any knowledge of the internal workings of a product, it is very difficult for them to make purchasing decisions based on such properties. This leads to "bad products driving out good ones".[56] While *information asymmetry* applies to both professional users (such as critical infrastructure) as well as consumers, it is in particular the case for consumers. As a result, manufacturers cannot gain a competitive advantage from investing in the security of their products, such as by adopting a SDLC.

Cybersecurity as a potential barrier to fast market entry (first-mover advantage)

Not only do manufacturers lack positive incentives to invest in security, emphasising product security can sometimes even be detrimental to the success of an undertaking: In a competitive market, companies can only bear additional marginal cost stemming from cybersecurity if their competitors are taking investments in cybersecurity equally seriously, unless they can increase prices because users value the integration of additional security properties. Hardware and software, however, are often characterised by the presence of strong network effects and economies of scale, making markets for products with digital elements a *winner takes it all* economy.

Due to the fast-paced nature of markets for products with digital elements, manufacturers are usually trying to bring new products or features for existing products onto the market as quickly as possible, prioritising feature development and compatibility with existing products, treating the development of security properties as an afterthought:[57] "From the economic perspective of the manufacturers, there are less benefits in strongly securing IoT devices compared to the benefits that arise from shorter development cycles omitting these security measures."[58] Nothing epitomises the fast market entry approach more than the motto that Facebook had adopted in its early years of development: *Move fast and break things*.

Securing products comes at a cost

While it is possible to improve the security of products through investment, companies tend to shy away from the costs associated with building a SDLC. The cost associated with improving product security depends on both the maturity of the entity as regards cybersecurity as well as the level of ambition. According to a recent study on the cost of required security, the cost associated with the additional effort made to improve the security of software products is at least 19 % of the development costs, depending on the security objectives to be achieved.[59]

Traditionally, researchers believed that rational manufacturers should invest in cybersecurity (such as by setting up a SDLC), as it would be cheaper to prevent vulnerabilities in the first place than to fix them at a later stage (delayed issue effect).[60] More recently, however, researchers have begun to challenge this notion, bringing forward new evidence suggesting that patching security holes in a product at a later stage is no more expensive than resolving security issues

[56] Ross Anderson (2001): "Why Information Security is Hard – An Economic Perspective", *Seventeenth Annual Computer Security Applications Conference*, p. 6.
[57] Morgner, Mai, Koschate-Fischer et al (2020): "Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products", *2020 IEEE Symposium on Security and Privacy (SP)*, p. 429.
[58] Morgner and Benenson (2018), p. 4.
[59] Elaine Venson (2021): "The Effects of Required Security on Software Development Effort", A Dissertation Presented to the Faculty of the USC Graduate School University of Southern California.
[60] Tim Menzies, William Nichols, Forrest Shull, Lucas Layman (2017): "Are Delayed Issues Harder to Resolve? Revisiting Cost-to-Fix of Defects throughout the Lifecycle", *Empirical Software Engineering, Volume 22, Issue 4 August 2017*, pp 1903-1935.

early during development.[61] This further substantiates the view that, given the cost of cybersecurity, manufactures have no natural incentive to develop secure products.

2.2.2. Driver 2: Piecemeal coverage of cybersecurity in EU policies

Currently there are no specific cybersecurity requirements comprehensively and systematically applicable to all products with digital elements, hardware or software, accessing the internal market. Cybersecurity of software (embedded in hardware and upload-able or of generic use, i.e. standalone[62]) in particular, of key importance for cybersecurity policies, is the least regulated even at the level of sector- or product-specific legislation with limited scope.

In order to effectively ensure the security of products as per the problems identified, **comprehensive and systematic cybersecurity requirements** applicable to all digital products, should entail as key minimum elements, that: (i) **cybersecurity is factored in the design and development** of the digital products and that due diligence is exercised by manufacturers on security aspects when designing and developing their products, (ii) **transparency** is ensured on cybersecurity aspects that need to be made known to customers and (iii) **security support (updates and handling of vulnerabilities)** are provided after the placement on the market.

Nonetheless, there is a small set of EU legal acts providing for product-related cybersecurity requirements. This is the case of the Radio Equipment Directive (RED)[63] together with a recently adopted delegated regulation,[64] which covers IoT devices outfitted with a radio interface, or the Medical Devices Regulation (MDR),[65] which covers both tangible medical products as well as software. In addition, there are a few European product laws that provide some rules regarding the cybersecurity of products, albeit only in a *partial* manner, such as the Toy Safety Directive (TSD).[66]

However, most hardware, such as wired IoT devices or computer components, including chipsets, memory chips or processors, as well as the vast majority of software products, such as operating systems, user applications, server software or software libraries, are not covered by any European legal act dealing with their cybersecurity.

The exploratory study contracted by the Commission and conducted in 2020-2021 to assess the need for horizontal cybersecurity requirements for products with digital elements, conducted a **gap analysis[67]** comparing the cybersecurity objectives set out in the Cybersecurity Act (Article 51)[68] against the identified cybersecurity-relevant requirements of **37 pieces of EU legislation** concerning products with digital elements. This included all legislation related to the New Legislative Framework (NLF), as well as legislation with a strong link with cybersecurity and data protection, which can affect indirectly and to a limited extent manufacturers (e.g. the eIDAS Regulation, General Data protection Regulation (GDPR), the NIS Directive, RED and GPSD).[69]

The NLF is a package of measures that streamline the obligations of manufacturers, authorised representatives, importers and distributors, improve market surveillance and boost the quality of conformity assessments. It also regulates the use of CE marking and creates a toolbox of

[61] Tim Menzies et al. (2017): pp 1903-1935.
[62] i.e. software that can be purchased by end users separately, such as operating systems; mobile apps; desktop applications; video games.
[63] Directive 2014/53/EU (RED).
[64] C(2021) 7672 final supplementing RED, with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of RED.
[65] Regulation (EU) 2017/745, (MDR).
[66] Directive 2009/48/EU, (Toy Safety Directive).
[67] Section 2.2 of the final report of the *Study on the need of Cybersecurity requirements for ICT products*, pages 52-61.
[68] To date, the Cybersecurity Act provides the most comprehensive set of cybersecurity requirements in EU law.
[69] The gap analysis used as a basis the Cybersecurity Act because it is one of the most recent, up-to-date, and relevant EU legislation that covers cybersecurity for products with digital elements at broad spectrum. The cybersecurity objectives of Article 51 also provide a comprehensive list of high-level cybersecurity requirements for products with digital elements, such as protection against unauthorised access or disclosure of information, or verification, or to follow the security by default principle.

measures for use in product legislation. This framework was introduced in 2008 to depart from the 'old approach' where technical legislation was going into great detail, usually motivated by a lack of confidence in the rigour of economic operators on issues of public health and safety.

The gap analysis concluded that the **current EU legislative framework does not cover all security objectives**, that legislation related to the **NLF does not address fully the cybersecurity requirements** for products with digital elements and that there are different levels of granularity of cybersecurity requirements in the legislation in scope. In addition, the study concluded that requirements regarding software are very rarely covered by such legislation.[70] For more details on existing European legislation, see *section 1* in *Annex 5*.

As a result of the regulatory gaps described, no piece of EU legislation requires currently comprehensive cybersecurity requirements for all products with digital elements. While there is a variety of international standards concerning several aspects of product cybersecurity (consumer IoT, assurance of security throughout lifecycle or vulnerability handling, access control, etc.), there are no harmonised European standards for products with digital elements across sectors (*see Annex 14*).

A detailed regulatory gap analysis can be found in *Annex 13*.

2.2.3. Driver 3: Manufacturers do not provide information on security properties and vulnerabilities

Markets for products with digital elements exhibit strong information asymmetries.[71] This is in particular for closed source products,[72] but also applies to open source products,[73] given the high degree of complexity of products with digital elements. Against the backdrop of a user base that for the most part lacks the skills to evaluate the security properties of products with digital elements, manufacturers in products with digital elements markets are facing a *moral hazard*, being incentivised to further deprioritise product security and transferring the risk onto users.[74] This leads to a situation in which manufacturers compete with one another on product features, such design or usability, but not on advertised security properties. In many cases, the information provided by manufacturers does not even allow proficient users or companies, such as operators of essential services under the NIS Directive, to compare security requirements with security properties and to make informed purchasing decisions about products.[75] This is not only true when it comes to products with digital elements developed for end-users, but also with regard to intermediate software components used by other software manufacturers to build final products.[76]

Asked in the public consultation if they agreed with the statement that *"There is sufficient and clear information made available on the cybersecurity properties of products with digital elements"*, participants gave an average rating of 2.50 (on a scale from 1 to 5), with consumer organisations giving a rating of only 1.33, users (business and consumers) giving a rating of 2.34, hardware manufacturers rating the information they provide with 2.85. SMEs and organisations representing SMEs in general rated it at 2.4 and 2.6 out of 5, similar to the average, with a slightly higher rating of 3.00 for organisations representing SME manufacturers, and those representing SME users rating it at 2.0.

---

[70] Study supporting the Commission preparatory work for the Cyber Resilience Act – N° 2019-0024.
[71] Jeffrey Vagle (2017): "Cybersecurity and Moral Hazard", *Stanford Technology Law Review*, Vol. 23, 2020, p. 85.
[72] Closed source refers to software for which the manufacturer does not disclose the source code, making it extremely difficult to assess the functionality and security properties of a product.
[73] Open source refers to software for which the manufacturer discloses its source code to the public, allowing other manufacturers and security researchers to analyse the inner workings of a programme as well as its security properties.
[74] Jeffrey Vagle (2017): p. 87.
[75] Dutch Safety Board (2021): *"Vulnerable through software. Lessons resulting from security breaches relating to Citrix software",* p. 89.
[76] Khan and Han (2006): "Assessing Security Properties of Software Components: A Software Engineer's Perspective", *Australian Software Engineering Conference (ASWEC'06)*, p. 1.

2.2.4. Driver 4: Manufacturers do not provide information on secure use

Apart from not disclosing relevant information about the security properties of products with digital elements, manufacturers often also fail to provide information helping users employ products in a secure manner, such as by including information on secure use in the manual or installation instructions. A recent survey of IoT device manufacturers revealed that only 43 % of manufacturers provide information on how users can change default passwords and only 26 % of manufacturers provide additional advice on how to protect their products from cybersecurity breaches.[77]

2.2.5. Additional drivers not addressed by this intervention

In addition to the drivers listed above, there are a number of additional problem drivers that have an impact on the security of products with digital elements as well as on the understanding of users as regards such products. However, given the nature of the product-related intervention considered, these additional drivers would not necessarily be addressed directly.

- **Lack of bargaining power of users:** Products with digital elements markets are often characterised by the presence of a few large manufacturers due to *economies of scale* and *vendor lock-in*, the latter being the result of a lack of compatibility between hardware and software platforms. As a result, users of products with digital elements lack the bargaining power necessary to ensure that manufacturers develop products matching the security needs of specific users.
- **Lack of qualified security professionals:** Manufacturers of products with digital elements often struggle to hire qualified security professionals: For example, the gap in cybersecurity professionals in Europe amounted to 199 000 in 2020. The Union is trying to address the skills gap through a variety of measures, including funding through the Digital Europe Programme.
- **Lack of cybersecurity awareness and skills of users:** Studies show that users often lack even the most basic cybersecurity skills. While this applies in particular to consumers, who are often not even familiar with basic internet security terminology, it also affects businesses and other organisations: For instance, only half of business leaders and only a third of their employees acknowledge the risk that cybercrime poses to their organisations.

More details on additional drivers identified can be found in *section 2* of *Annex 5*.

2.3. Consequences of the problems identified

2.3.1. *Consequence 1: Increased number of cybersecurity incidents with material and non-material harm to citizens and companies*

The **importance and impact of cyberattacks** have increased dramatically in recent years. On the one hand, both companies and consumers are growing more dependent on products with digital elements. This trend has been exacerbated by the COVID-19 crisis, which gave rise to widely spread telework and accelerated the digitisation of society. In addition, critical infrastructure as well as manufacturers are increasingly connecting their industrial control systems (ICSs) to the Internet.[78] On the other hand, cyberattacks are sharply increasing and they are used as an economic and geopolitical weapon.[79]

---

[77] Rodríguez et al (2021) "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, for a more detailed discussion of IoT consumer device security, p. 9.

[78] https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/

[79] Cyberattacks are performed by criminal groups as well as increasingly by nation state actors and other state-sponsored groups. Motives are manifold and include personal gain, cyber terrorism, signals intelligence and espionage, intellectual property theft as well as cyber warfare, often blending with conventional warfare.

The 2020 Annual Cost of a Data Breach Report of the Ponemon Institute estimates that the average **cost of a data breach** for individual businesses was EUR 3.5 million in 2018, which is an increase of 6.4 % over the previous year.[80] Such costs include, but are not limited to, getting systems and manufacturing processes back online, managing the reputational fallout, paying a ransom, recovering or compensating for lost or stolen data, and cleaning, reinstalling or replacing affected hardware. In many cases, it takes months for companies to fully recover from an incident.

As incidents affect the availability, integrity, authenticity and confidentiality of services, they often affect customers (e.g. a service might become unavailable or sensitive customer data might be stolen) and sometimes propagate across organisations and supply chains throughout the internal market, generating considerable costs. For example, ransomware attacks alone are estimated to have cost the world roughly USD 20 billion in the year 2021. Statistically speaking, every 11 seconds another organisation is hit by a ransomware attack.[81]

Supply chain attacks represented a major problem in recent years: cybercriminals introduce malicious code into legitimate products with digital elements for the purpose of attacking the users of such products.[82] One of the most prominent recent examples is the SolarWinds attack in 2020.

Vulnerabilities and badly configured systems not only affect the security of organisations but also have a major impact on consumers. Impacts can be financial, as well as related to privacy or health. For instance, when it comes to financial harm, certain types of malware infect the devices of citizens with the goal of collecting online banking credentials and secretly executing payments.[83] Incidents can also have an impact of the safety of citizens. For example, cybersecurity incidents in hospitals have been found to lead to a small increase in mortality rate.[84] In a number of instances, IoT consumer devices have been hacked to track the lives of citizens.[85]

A phenomenon of particular relevance to consumers is the hacking of IoT devices for the purpose of integrating them into a *botnet*, a larger network of devices stretching across the internal market and beyond, controlled by a malicious actor and used to conduct so-called DDoS attacks[86] affecting the availability of services provided by organisations, such as critical infrastructure, and to send out unwanted spam messages to email users. Cross-border botnets create significant negative externalities, as it is usually not the device owners that have to bear the cost of device abuse but rather the victims of DDoS attacks or the recipients of spam.[87] It is estimated that an individual small company targeted by a DDoS attack can face costs up to USD

[80] Annual Cost of a Data Breach Report, 2020, conducted by the Ponemon Institute, and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries.
[81] https://www.dataprivacyandsecurityinsider.com/2020/02/ransomware-attacks-predicted-to-occur-every-11-seconds-in-2021-with-a-cost-of-20-billion/.
[82] This once again raises the attention around supply chain attacks, which are often cross-border in nature. See https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
[83] For example, between 2007 and 2009 the ZeuS/Zbot trojan has infected computers globally by tricking users into downloading malicious content and by exploiting vulnerabilities. The crime group responsible for the trojan has allegedly stolen around 70 million USD, predominantly in the United States and United Kingdom. See Zhong et al (2015): "Stealthy Malware Traffic – Not as Innocent as It Looks", *2015 10th International Conference on Malicious and Unwanted Software*.
[84] Choi and Johnson (2017): "Do Hospital Data Breaches Reduce Patient Care Quality?", *Workshop on the Economics of Information Security 2017*.
[85] In 2019 household cameras sold by the company Ring were accessed, allowing hackers to observe citizens at home. In one case, an attacker addressed a child using a camera's speakers. In 2021, a group of hackers gained access to the footage of Verkada cameras deployed in organisations, such as Tesla's warehouses and factories, Cloudflare, health clinics and psychiatric hospitals.
[86] A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.
[87] See Rodríguez, Noroozian, van Eeten and Gañá (2021): "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, for a more detailed discussion of IoT consumer device security.

120 000, while for larger companies the cost can go as high as USD 2 million.[88] In 2021 alone cybercriminals were able to leverage hacked devices and launch 9.75 million DDoS attacks worldwide.[89]

Generally speaking, entities across all economic sectors tend to fall victim to cybersecurity attacks. This is first and foremost explained by the fact that "in many cases the threats manifest themselves by exploiting vulnerabilities in underlying ICT systems that are being used in a variety of sectors"[90]. Nonetheless, certain sectors are more affected than others: According to the EU's cybersecurity agency (ENISA), public administrations, digital service providers, healthcare and finance are the sectors experiencing the highest number of incidents, while sectors such as water utilities, postal and courier services, space and semiconductors are the least affected.[91] These differences are explained by the relative economic importance of certain sectors as well as by the maturity of organisations when it comes to cyber resilience, an issue being addressed by the revision of the NIS Directive.

Respondents to the public consultation have overall rated the consequences of cybersecurity incidents as very high. SMEs consistently rated on average the material consequences of cybersecurity incidents higher than other organisations.[92]

2.3.2. *Consequence 2: Increased cost to society to mitigate cyber risks*

In addition to the costs following an incident, businesses and other organisations are also forced to invest significantly into incident prevention, handling and mitigation as a result of non-secure products with digital elements. Such investments include taking out cybersecurity insurance or putting in place entire company departments dedicated to security, such as cybersecurity incident response teams (CSIRTs) or security operations centres (SOCs). According to the Commission's impact assessment for the revision of the NIS Directive, the average ICT security spending of companies in 2020 is of approximately 9.14 % of their ICT spending.[93]

In the public consultation, both consumers as well as respondents identifying themselves as users agreed with the statement that *"The user bears additional costs due to highly priced cybersecurity insurance"*, rating it at 4.50 and 3.48 respectively (on a scale from 1 to 5). Similarly, consumers and users agreed with the statement that *"The user bears additional costs due to the need to deploy highly priced technical security solutions"*, rating it at 3.67 and 4.03 respectively. In particular SMEs in their role as users agreed with the two statements (3.80 and 4.20 respectively).

2.3.3. *Consequence 3: Reduced uptake of digital solutions*

Finally, lacking cybersecurity also creates *opportunity costs* for businesses, governments and society as whole, when modern technologies are not deployed as quickly as possible for fear of being unable to manage the risks associated with them. This may seem counterintuitive given the recent substantial increase in digitisation caused by the pandemic. But irrespective of the exceptional circumstances in recent years, security concerns are considered as one of the main barriers to the adoption of products with digital elements.[94] In fact, security concerns are one of

[88] https://www.bulletproof.co.uk/industry-reports/2019.pdf, p. 20.
[89] https://www.helpnetsecurity.com/2022/03/28/ddos-attacks-2021.
[90] ENISA (2021): "ENISA Threat Landscape 2021. April 2020 to mid-July 2021", p. 11.
[91] ENISA (2021), p. 13.
[92] The consequences regarded the financial cost of implementing measures to respond to a cybersecurity incident (3.81; 4.2 for SMEs), the financial cost of disruption (3.96; 4.6 for SMEs), the reputational damage of the affected entity (3.96; 4.2 for SMEs), the negative impact on the security of the economy and society as a whole (3.67; 4.4 for SMEs) and the damage to fundamental rights, such as privacy, data protection and consumer protection (3.80; 4 for SMEs). In comparison, the negative impact on health and life (2.71) and on the environment (2.31) were regarded as less severe.[92] This was also the case for SMEs.
[93] SWD(2020) 345 final, IA accompanying the NIS2 proposal, p. 71.
[94] This is the case in the health sector, where security concerns are a major barrier to the uptake of new technology. See here.

the main reasons why decision makers are shying away from investments in IoT solutions.[95] A reduced uptake of digital solutions can have a negative impact on innovation, efficiency gains and, as a result, economic growth.

2.3.4. *Consequence 4: Risk of emergence of internal market fragmentation*

While only few Member States have so far introduced measures to regulate the security of products with digital elements at national level (both Germany and Finland have introduced labelling schemes, see *section 6.3*), the scale of the problems associated with insecure products with digital elements could in the future lead to targeted product-specific interventions at national level. The Council considers the security issues associated with products with digital elements as a matter of urgency and has repeatedly called upon the Commission to propose regulation in this area. Member States are aware that, given the impact on the internal market, measures need to be taken at EU level. In the absence of EU regulation however, they are likely to take further action, within then limits allowed by the treaties. This could be the case particularly to achieve objectives in the areas of safety, health, environment and consumer protection, these being areas where national regulations of this sort could be acceptable without being considered a breach of free movement of goods in the internal market. This could lead to a situation in which manufacturers would be facing an unsystematic approach to product security across the internal market. This could result in internal market fragmentation with negative consequences for the cost-effectiveness and competitiveness of European hardware and software manufacturers (see *section 6.3*). In the public consultation, respondents rated the question *"To what extent do you agree that there is a risk of increasing costs and legal uncertainty for market stakeholders, in the absence of an EU initiative?"* with 4.38 out of 5 (with 5 indicating that they fully agree). SMEs responded with 4.4 out of 5, and organisations representing SMEs with 4.5.

Finally, in absence of harmonised rules, users, such as critical infrastructures obligated under the revised NIS Directive to take their supply chain security more seriously, may start putting in place diverging contractual requirements for manufacturers of products with digital elements.

2.4. How likely are the problems to persist?

There have been numerous efforts to improve the cybersecurity of products with digital elements both by academia and by the manufacturing and development community. For instance, new programming languages, such as Rust or Go, have been developed that minimize the risk of certain types of vulnerabilities, such as memory corruption. Several mostly large manufacturers have started adopting a SDLC with a view to improve software and hardware security. As a result, security software, such as static and dynamic testing tools, has become available on the market, helping manufacturers to verify the security of computer code. Moreover, some manufacturers of products, such as operating systems, browsers and routers, are outfitting their products with automated updating features, ensuring that also inexperienced users can benefit from the latest security updates.

In addition, the Cybersecurity Act, which came into force in 2019, provides for the possibility to certify, on a voluntary basis, ICT products, services and processes. A number of product-specific international standards have also emerged, such as ETSI's Consumer Mobile Device Protection Profile, standards for industrial automation and control systems,[96] or a set of guidelines released by the Open Web Application Security Project (OWASP).

Some of the problem drivers described in the previous section may diminish in the future. For example, the labour market may adjust and provide manufacturers with more qualified security professionals, either as a result of market forces or following government measures. Similarly, as a result of awareness raising campaigns and adapted school curricula, users could become more

[95] See the IoT Large Scale Pilots eBook, p. 11.
[96] Such as IEC 62443 .

aware of cybersecurity risks and more proficient in using products with digital elements securely.

However, while some of the recent market developments and standardisation and certification efforts are steps in the right direction, most of the problem drivers are very unlikely to disappear, given that they are the **direct result of persistent structural market failures**. The lack of incentives for manufacturers to take the cybersecurity of their products seriously will persist in the presence of negative externalities and information asymmetries, but also against the backdrop of a fast-paced industry that rewards early market entry above everything else. Given that existing standards are voluntary and non-comprehensive, manufacturers have little incentive to apply them. In addition, while new supply chain security requirements for critical infrastructure and other essential entities under the reviewed NIS Directive[97] will help put pressure on hardware and software manufacturers, business users and other organisations, such as public administrations, will continue to lack negotiating power in more concentrated products with digital elements markets.

While there have been various attempts within the market to improve the security of products with digital elements, the overall assessment that many products with digital elements are highly vulnerable is unlikely to change without government intervention. A recent study on software vulnerabilities has concluded that *"in 15 years, the vulnerability landscape hasn't changed; through the lens of the metrics in this paper we aren't making progress."*[98] As a result, regulators have little reason to believe that the situation will substantially improve without regulatory intervention.

In the absence of European legislation, Member States are likely to introduce national regulations laying down security requirements on such categories of products, within the limits allowed by EU law. While national intervention could contribute to reducing the problem of low product security, it would inevitably also lead to **internal market fragmentation**, preventing manufacturers on an otherwise global products market from providing hardware and software solutions across the internal market in a cost-effective manner (see *section 6.3* for more details).

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

This intervention will be based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The measures must be intended to improve the conditions for the establishment and functioning of the internal market and must genuinely have that objective, actually contributing to the elimination of obstacles to the free movement of goods or services, or to the removal of distortions of competition.

Article 114 TFEU may be used as a legal basis to prevent the occurrence of these obstacles resulting from diverging national laws and approaches on how to address the legal uncertainties and gaps in the existing legal frameworks.[99] Furthermore, the Court of Justice has recognised that applying heterogeneous technical requirements could be valid grounds to trigger Article 114 TFEU.[100] The present intervention would aim to improve the internal market's functioning by streamlining and supplementing existing rules.

[97] See Article 18 (2) (d) in COM/2020/823 final, NIS2 proposal.
[98] Gueye and Mell (2021), p. 6.
[99] CJEU Judgment of the Court (Grand Chamber) of 3 December 2019, Czech Republic v European Parliament and Council of the European Union, Case C-482/17, paras. 35.
[100] CJEU Judgment of the Court (Grand Chamber) of 2 May 2006, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union, Case C-217/04, paras. 62-63.

The current EU legislative framework applicable to products with digital elements is based on Article 114, and comprises several pieces of legislation, including on specific products and safety-related aspects or general legislation on product liability. However, it covers only certain aspects linked to the cybersecurity of tangible products with digital elements and, as applicable, software embedded in these products.

As explained in more detail in *section 6.3*, at national level, Member States are starting to take national measures requiring manufacturers of products with digital elements to enhance their cybersecurity. At the same time, the cybersecurity of products with digital elements has a particularly strong cross-border dimension, as products manufactured in one country are often used by organisations and consumers across the entire internal market. Incidents that initially concern a single entity or Member State often spread within minutes across organisations, sectors and several Member States.

The various acts and initiatives taken so far at EU and national levels only partially address the problems identified and risk creating a legislative patchwork within the internal market, increasing legal uncertainty for both manufacturers and users of these products and adding unnecessary burden on companies to comply with a number of requirements for similar types of products. Therefore, the envisaged intervention would harmonise and streamline the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements and avoid overlapping requirements stemming from different pieces of legislation. A horizontal regulatory intervention on cybersecurity of products would do away with legal uncertainty on these aspects triggered by a patched approach taken in various product-specific or general product-related pieces of legislation. It would create greater legal certainty for operators and users across the Union, as well as a harmonisation of the European single market, creating more viable conditions for operators aiming at entering the EU market.

3.2. Subsidiarity: Necessity of EU action

The strong cross-border nature of cybersecurity in general and the growing risks and incidents, which have spill-over effects across borders, sectors and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone. Taking into account the global nature of markets for products with digital elements, Member States face the same risks with respect to the same product with digital elements on their territory. For example, a recent study on infected IoT products across the internal market has revealed that it is the same nine manufacturers in each country that are responsible for placing the highest number of IoT devices on the market that have been infected as a result of vulnerabilities, concluding that "international collaboration among regulators in various countries is a feasible path. This would not only bundle scarce resources on the side of governments, but is also more likely to influence manufacturer behaviour through collective action. An obvious starting point would be coordination at the level of the European Union."[101]

An emerging patchy framework of potentially diverging national rules also risks hampering an open and competitive single market for products with digital elements. Some Member States, such as Germany and Finland have already taken first (non-binding) measures to improve the security of products with digital elements (see *section 6.3*). National approaches in addressing the problems, and in particular approaches introducing mandatory requirements, will only create additional legal uncertainty and legal barriers. Companies could be prevented from seamlessly expanding into other Member States, depriving users of the benefits of their products.

[101] Rodríguez et al (2021): "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, for a more detailed discussion of IoT consumer device security,
p. 8

Given the lack of negotiation power of individual users on a global products market with large multinational manufacturers (see *section 2.2.5*), regulation at national level would not be effective. In a 2021 report, the Dutch Safety Board concluded that the products with digital elements market "can hardly be influenced by users in the Netherlands alone. Influencing such a global market requires a larger power block, for example at EU or UN level, or based on joint actions by end users."

Joint action at EU level is therefore necessary to establish a high level of trust among users, increasing the attractiveness of EU products with digital elements. It would also benefit the (digital) single market and internal market in general by providing legal certainty and achieving a level playing field for manufacturers of products with digital elements. Ultimately, as referred to in *section 1,* the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture[102] call upon the Commission to propose, by the end of 2022, common cybersecurity requirements for connected devices.

3.3. Subsidiarity: Added value of EU action

The objectives of the initiative can be better achieved at Union level so as to avoid a further fragmentation of the single market into potentially contradictory national frameworks. A single framework regarding cybersecurity requirements for products with digital elements would provide legal certainty and avoid overlapping or contradictory requirements stemming from different pieces of legislation. Harmonised EU requirements would facilitate compliance for manufacturers of products with digital elements and create more viable conditions for operators aiming at entering the EU market.

Users' trust that products with digital elements acquired in any Member State comply with a harmonised set of requirements would increase their trust in and demand for these products. Given the global and cross-border nature of the digital market and the internet, the intervention would reduce negative cross-border spill-overs and costs to society linked to mitigating risks of non-secure products.

As regards the **proportionality** of the intervention, the measures in the policy options considered would not go beyond what is needed to achieve the general and specific objectives and would not impose disproportionate costs. More specifically, the intervention considered would ensure that products with digital elements would be secured throughout their whole life cycle and proportionally to the risks faced through objective-oriented and technology neutral requirements that remain reasonable and generally corresponding to the interest of the entities involved.

[102] Council conclusions on the development of the European Union's cyber posture (2022).

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

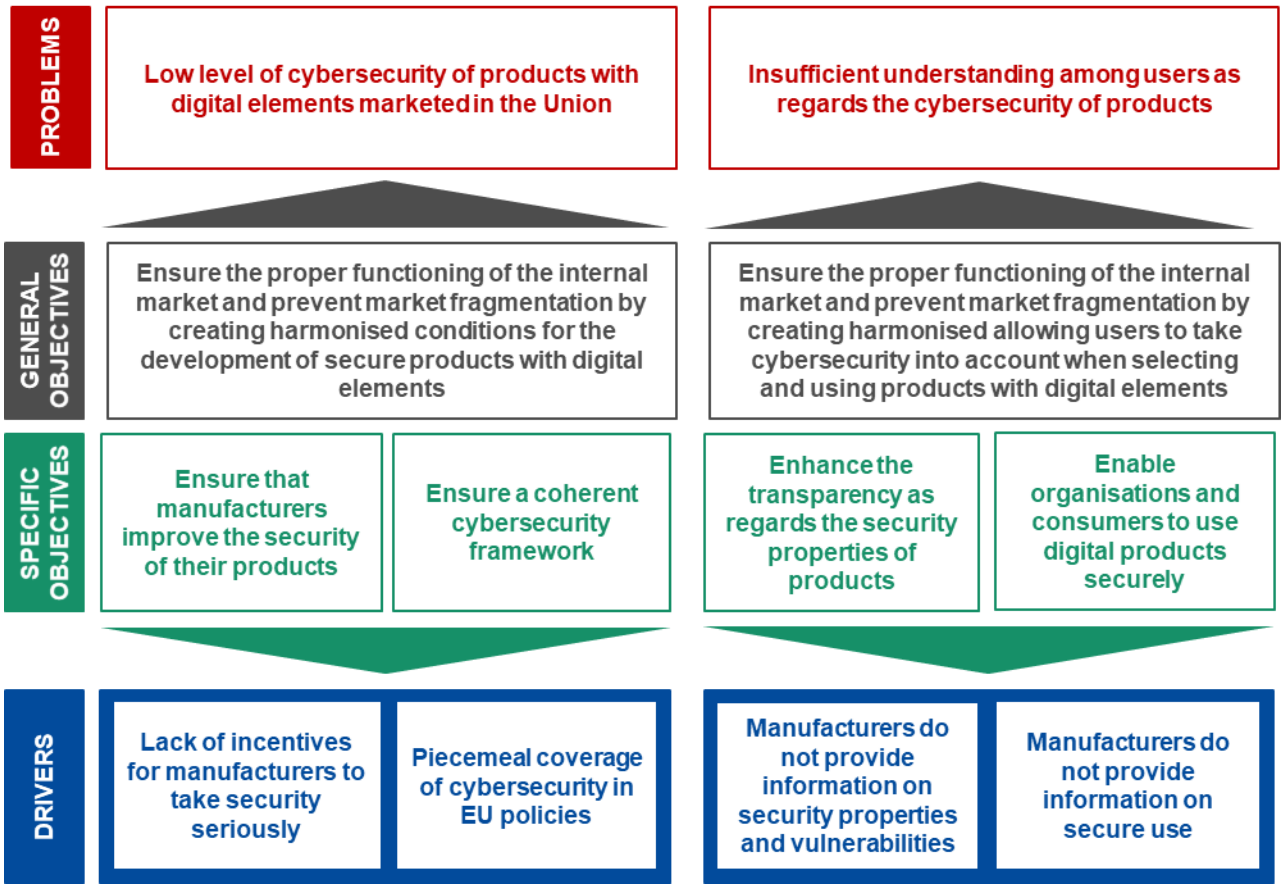

Figure 2: Intervention logic

4.1. General objectives

Based on the main problems identified in the *section 2.1*, the main objectives of the intervention should be as follows:

General Objective 1 (GO1): Ensure the proper functioning of the internal market and prevent market fragmentation by creating harmonised conditions for the development of secure products with digital elements.

The intervention should ensure that hardware and software products are released to the market with fewer vulnerabilities and that manufactures take the security seriously throughout a product's entire life cycle, in particular by providing timely security updates. In addition, it is important that manufacturers prevent malicious actors from tampering with production code.

General Objective 2 (GO2): Ensure the proper functioning of the internal market and prevent market fragmentation by creating harmonised allowing users to take cybersecurity into account when selecting and using products with digital elements.

The intervention should ensure that both consumers as well as business users and other organisations are able to select products whose security properties match their security requirements. In addition, measures should be taken to support users in operating technical in a secure manner.

4.2. Specific objectives

Based on the problem drivers identified in *section 2.2* and with a view to reaching the two general objectives defined above, the specific objectives of the intervention should be as follows:

To address the problem of low level of cybersecurity of products with digital elements marketed in the Union:

SPO1 Ensure that manufacturers improve the security of their products with digital elements since the design and development phase and throughout the whole life cycle of those products

SPO2 Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software manufacturers

To address the problem of insufficient understanding among users as regards the cybersecurity of products:

SPO3 Enhance the transparency as regards the security properties of products with digital elements

SPO4 Enable organisations and consumers to use products with digital elements securely

As referred to in *section 2.2.5,* there are certain additional problem drivers that will not be addressed by the proposed intervention. This is not to say that the intervention will have no impact at all on these drivers (see *section 6.7*).

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

This section presents the policy options, including the baseline scenario, that have been considered for addressing the problems identified in *section 2* and meeting the objectives set out in *section 4*.

Problem drivers	**Specific policy objectives**					**Policy options**			
		PO1 (soft law)	**PO2** (ad-hoc interv.)	**PO3** (mixed appr.)		**PO4** (horiz. interv.)			
						PO4 a) (horiz. interv. only critical software)		**PO4 b)** (horiz. interv. all software)	
				PO 3 i)	**PO 3 ii)**	**PO 4 a) i)**	**PO 4 a) ii)**	**PO4 b) i)**	**PO4 b) ii)**
DR1: Lack of incentives for manufacturers to take security seriously	**SPO1:** Ensure that manufacturers improve the security of their products with digital elements since the design and development phase and throughout the whole life cycle of those products	—Communications, guidance and recommendations for supply side stakeholders, including on non-embedded software —Recommendation on public procurement of products with digital elements — Development of additional European cybersecurity certification schemes	—Amendments to *existing* product specific legislation —Integrate cybersecurity into *future* product-specific NLF legislation	—Horizontal regulatory intervention for tangible products with digital elements (excluding non-embedded software) —A potential legal act on non-embedded software at a later stage (staggered approach)		—Horizontal regulatory intervention for a broad scope of **tangible and only critical intangible products** with digital elements (including non-embedded software)		—Horizontal regulatory intervention for a broad scope of **tangible and intangible products** with digital elements (including non-embedded software)	
				— self-assessment by default for all products covered	— third-party assessment for a narrow share of critical tangible products	— self-assessment by default for all products covered	— third-party assessment for a narrow share of critical tangible and intangible products	— self-assessment by default for all products	— third-party assessment for a narrow share of critical tangible and intangible products
DR2: Piecemeal coverage of cybersecurity in EU policies	**SPO2:** Ensure a coherent cybersecurity framework								
DR3: Manufacturers do not provide information on security properties and vulnerabilities	**SPO3:** Enhance the transparency as regards the security properties of products with digital elements	*(partly included in the measures addressing DR1)*	*(partly included in the measures addressing DR1)*	Horizontal intervention to include transparency requirements for tangible products with digital elements on security properties		Horizontal intervention to include transparency requirements for both tangible and critical intangible products with digital elements on security properties		Horizontal intervention to include transparency requirements for both tangible and intangible products with digital elements on security properties	

DR4: Manufacturers do not provide information on secure use	**SPO4:** Enable organisations and consumers to use products with digital elements securely	*(partly included in the measures addressing DR1)*	*(partly included in the measures addressing DR1)*	Horizontal intervention to include transparency for tangible products with digital elements requirements on secure use		Horizontal intervention to include transparency requirements for both tangible and critical intangible products with digital elements on secure use	Horizontal intervention to include transparency requirements for both tangible and intangible products with digital elements on secure use

Table 1: Problem drivers, specific objectives and policy options

5.1. What is the baseline from which options are assessed?

5.1.1. The relevant EU markets

A horizontal regulatory intervention would lay down requirements for some or all products with digital elements marketed in the Union (with the broadest scope under policy option 4). Requirements would not only cover the final product with digital elements (e.g. a smart phone), but also their components, both for hardware and software. As a result, depending on the policy options, the initiative would have an impact throughout the entire digital supply chain, and provide users with a very high level of assurance regarding the security of products. *See also the illustrative example of smart phones in the description of options 3 and 4, section 5.2.*

The relevant markets include software and hardware products, which the policy options will impact to a different extent. Due to the absence of a consistent and comparable publicly available dataset on the dimension of the market for products with digital elements, certain proxy indicators have been used to assess the value of the relevant markets. The methodology and the market analysis is described in more detail in *Annex 3*. The analysis includes the value produced by both non-EU and EU companies in the EU market, while it was not possible to generate aggregated values for each of these two.

5.1.1.1. Software market

Based on the data gathered by a recent study which provided for a breakdown of the software and software-based services market,[103] the following categories can be identified: (*1) Software products;*[104] *(2) Software-related services;*[105] *(3) Cloud computing;*[106] *(4) Games.* The present analysis is focused on software products (including games) and does not explore the specific markets related to software services and cloud. This is because the latter would not be included in the scope of a potential horizontal regulation (policy options 3 and 4), since only products (and hence software as a product) would be included in the scope and not services.[107]

The proxy indicator used to assess the dimension of the software market is based on a subset of NACE 2 activities of the Information and Communication sector (see *Annex 3*).

The proxy indicates that, in 2019, the **production value** of the EU-27 software development amounted to over **EUR 236 billion**.[108] During the same year, the sector recorded a **turnover** of EUR 265 billion with a total **number of enterprises** of 365 759.[109]

In terms of **number of companies,** the software industry is almost entirely composed of **SMEs**. Whereas the total number of enterprises for the selected sample amounted to 341 781 in 2019, the number of SMEs operating in the software market in the same year reached 340 918, accounting for 99.7 % of the total.[110] However, when looking at the **turnover generated by SMEs** in the software market for sample countries, it **accounts for 41 %** of the EUR 305 444

[103] https://op.europa.eu/en/publication-detail/-/publication/480eff53-0495-11e7-8a35-01aa75ed71a1
[104] including infrastructure software & platforms, application software products; excluding SaaS.
[105] including application-related project services, application management, application hosting, infrastructure-related project services, infrastructure outsourcing; excluding cloud services.
[106] paid web-based services consisting of IaaS, PaaS, SaaS.
[107] Furthermore, software products not sold on the market, i.e. in-house software development (i.e. resulting in products that are not distributed externally as software products), were not included in the analysis.
[108] This data appears to be consistent with other estimations. For instance, the software development market which includes writing, modifying and supporting computer code, databases and webpages is estimated to amount to 255 billion. https://www.ibisworld.com/eu/industry/software-development/3595/
[109] EUROSTAT. Annual detailed enterprise statistics for services. The data is under evaluated due to the data for some countries due to confidentiality. The data for Estonia, Ireland, the Netherlands and Slovakia is missing for one of the NACE 2 indicators.
[110] 94 % of SMEs operating in the software market are micro enterprises (less than nine employee).

billion which shows the **important relative weight of big market players** that may constitute only 0.3 % of enterprises in the market but generate 59 % of revenue.

When referring to turnover, it is difficult to assess the share of the **revenues related to B2C and B2B**. Nevertheless, by looking at the German software market, it is possible to highlight that those revenues from software sales **rely heavily on B2B with 67.9 %** of revenue being driven from business. This split shows a high integration of the software market with other economic sectors that rely on software for their operations.[111]

The size of **embedded software** is valued at EUR 2.4 billion in 2020 and is expected to continue growing at a compound annual growth rate (CAGR) of 5.5 % from 2021 to 2027. **Non-embedded software** represents the **biggest part of the industry's sales**.[112]

Globally, the revenue in the software market[113] is projected to reach **USD 608.70 billion in 2022**, with nearly half of the revenue generated[114] in the United States. Most competitive software companies are from the United States followed by Asia. According to McKinsey, in 2020, there was no European company on the list of the world's ten most valuable software and software-enabled companies, and were only three among the top 20. Furthermore, over a third of the 100 most valuable companies in the United States came from the software sector, as did about a quarter of those in Asia. In Europe, that figure stood at just 7 %.[115]

5.1.1.2. Hardware market

To estimate the value of the hardware market, several proxies were explored based on Eurostat data in the study accompanying the impact assessment: the **ICT manufacturing sector – standard classification** (ICT-SC)[116] and the **extended classification** (ICT-EXT-ADJ). The latter covers more manufacturing sectors than those which are 'purely' digital. The estimates based only on the ICT manufacturing sector are under the real values of all products with digital elements placed on the Union market. At the same time, the estimates based on the extended classification are likely over the real value: The adjustment indicators used to estimate the weight of products with digital elements as compared to non-products with digital elements within the same category are an overestimation, since the proxy used for this adjustment considered the digital intensity of the manufacturing sub-sectors, which does not necessarily match the production of digital goods[117] (*see Annex 3*).

In 2019, the **production value** of the EU-27 ICT-SC amounted to **EUR 222 billion**. During the same year, the sector recorded a **turnover** of EUR 285 billion[118] with a total **number of enterprises** of 22 773.[119]

When considering the ICT-EXT-ADJ indicator, the production value of the EU-27 amounted to EUR 1 081 billion, the turnover to EUR 1 220 billion and the total number of enterprises of 249 513 in 2019. *As mentioned above, this would most likely be an overestimation.*

[111] Deloitte (2019). The German Technology Sector. From Hardware to Software & Services, p. 12.
[112] https://www.graphicalresearch.com/industry-insights/1988/europe-embedded-software-market
[113] including on-premise and cloud-enabled software.
[114] USD 303.10 billion in 2022.
[115] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/reversal-of-fortune-how-european-software-can-play-to-its-strengths
[116] Deloitte (2019), p. 7, but also Barefoot, K.; Curtis, D.; Jolliff, W.; Nicholson J.R.; Omohundro, R.; (2018). Defining and Measuring the Digital Economy – Working Paper. Bureau of Economic Analysis – US Department of Commerce. p. 47.
[117] For example, there can be businesses with high digital intensity that do not produce product with digital elementss.
[118] This data appears to be consistent with other estimations. For instance, Research and Markets assess the IT Hardware Market in Europe at USD 228.9 billion in 2020. The IT hardware market includes all physical components integral to computing such as computing, networking, security and server hardware. More info available at: https://www.researchandmarkets.com/reports/5350389/it-hardware-in-europe-market-summary
[119] Eurostat: Annual enterprise statistics for special aggregates of activities (NACE Rev. 2). [SBS_NA_SCA_R2]

The European ICT-SC manufacturing industry is almost entirely composed of SMEs. Whereas the total number of enterprises amounted to 22 773 in 2019, the **number of SMEs operating in the hardware market in the same year reached 22 119, accounting for 97.13 %** of the total.[120] However, when looking at the turnover generated by SMEs in the hardware market, it accounts for 21.9 % of the global turnover which shows the very important weight of larger companies that may constitute only 2.87 % of enterprises in the market but generate 78.1 % of revenue.

The **weight of the ICT manufacturing** on the overall European economy was stable over the past five years and still appears to be limited, amounting to 0.41 % in 2019.[121]

When referring to turnover, it is difficult to assess the share of the **revenues related to B2C and B2B**. Nevertheless, by looking at the German hardware market, it is possible to highlight that revenues from hardware sales were equally split between the B2B (48.1 %) and B2C (51.9 %) sectors in 2018. The reason behind this split is **the strong consumer business stream** connected to the sale of smartphones, laptops and general consumer electronics. This represents an important distinction with the software and services market where the B2B component appears to be predominant, accounting for more than two-thirds of the overall sales.[122]

5.1.1.3. Total market value

The global market for products with digital elements encompassing software and hardware has a total production value in Europe of EUR 458 billion and turnover of EUR 550 billion in 2019,[123] if the hardware market is considered as only including the elements of the ICT-SC indicator. The number of enterprises operating in this sector is **388 532,** when considering the limited scope of ICT-SC, with a vast majority being SMEs (99.58%).

Considering the extended classification (ICT-EXT-ADJ), these values are up to EUR 1317 billion in production value and EUR 1485 billion in turnover for 2019. The number of enterprises in this sector is **615 272**, with a vast majority being SMEs (99.58%). These estimates however may be overestimated since they rely on proxies of digital intensity and not production of digital goods per se.

Based on this data, under both indicators, SMEs account for about 34.4 % of the turnover generated in the market for products with digital elements for 2019. Aggregated indicators for the global market for products with digital elements in 2019 can be found in *Annex 3*.

5.1.2. Baseline scenario

The baseline scenario entails no common (i.e. horizontal) legislation to set cybersecurity requirements for products with digital elements.

As referred to in *sections 1 and 2.2.2.,* the current **EU framework applicable to products** comprises several pieces of legislation that cover only certain aspects linked to the cybersecurity of tangible products with digital elements and, where applicable, embedded software concerning these products. This legislative framework **was not conceived to tackle specifically the challenges linked to cybersecurity of products with digital elements**. It largely covers requirements for placing the products on the market, but not necessarily for the whole life cycle of products, which is crucial in the case of products with digital elements. The current legislation also fails to cover a variety of widely used hardware[124]. Moreover, **non-embedded software** is

[120] Source: EUROSTAT [SBS_SC_IND_R2]
[121] EUROSTAT. Percentage of the ICT sector on GDP. [TIN00074]. 82 % of SMEs operating in hardware market are micro enterprises (less than nine employee).
[122] Deloitte (2019). The German Technology Sector. From Hardware to Software & Services, p. 12.
[123] Second Interim Study Report N° 2019-0024 supporting the impact assessment.
[124] e.g. hardware not falling under the RED, such as wired-only hardware.

not currently addressed despite the major impact resulting from insecure non-embedded software. for a detailed gap analysis, see *Annex 13*.

As a significant first step towards increasing the level of cybersecurity of wireless devices, the **delegated act under RED**,[125] adopted in October 2021, aims to improve the cybersecurity of these devices on the European market by laying down new general requirements which manufacturers will have to follow in the design and production of the concerned products, constitutes. Non-embedded software is however not covered by these requirements. Furthermore, the act does not provide for duty of care for the whole life cycle of these products.

It can be assumed that, given the pace, spread and importance of digitization for all sectors of economy, any new product-related legislation in the NLF would include certain cybersecurity-related aspects. However, these would be product- and/or sector-specific and therefore would not be able to address cybersecurity risks in a targeted and comprehensive way. Leaving the integration of cybersecurity-related requirements only for certain product legislation would leave other categories of products not covered by such measures and possibly raise the risk of different and even diverging requirements stemming from separate pieces of legislation. This would lead to a **fragmented regulatory landscape, potential discrimination and legal uncertainty**, affecting the well-functioning of the internal market.

Maintaining this status quo would therefore mean that cybersecurity would remain only partially addressed in product-related legislation, while existing horizontal cybersecurity legislation, such as the NIS framework or the Cybersecurity Act, would not provide for the means to establish cybersecurity requirements for products with digital elements.

In the scenario of maintaining the status quo, the development of **European voluntary cybersecurity certifications schemes** would continue as foreseen, based on the Cybersecurity Act, implying a **voluntary conformity assessment**[126]. Manufacturers do not have a legal obligation to seek certification for their products. The proposal for the NIS2 Directive expected to enter into force before the end of 2022, with a transposition period of 21 months, provides for an empowerment for the Commission to adopt delegated acts specifying categories of essential entities shall be required to obtain a certificate under a European certification scheme. However, this would rather cover a limited category of products used in particular sectors and would therefore not be sufficient to address systematic cybersecurity-related issues of all products with digital elements, as described in *section 2*.

Other voluntary national practices and measures would continue, such as **voluntary labelling** measures of certain categories of products, as it is currently the case in few Member States. This can raise the risk of further fragmenting the internal market.

Finally, maintaining the status quo would entail no specific soft law or regulation at EU level as regards cybersecurity of **standalone software.**

At **national level**, Member States may develop targeted initiatives within the boundaries of European law to better protect their consumers. For example, Member States could put in place diverging security and transparency obligations for operating systems or virtual private network software, which is becoming increasingly popular since the beginning of pandemic.

[125] C(2021) 7672 final supplementing RED, with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of RED.

[126] There are currently three certification schemes at various stages of development under the European Cybersecurity Certification Framework on the basis of the Cybersecurity Act: (i) common criteria which concerns predominantly high assurance for components (smart cards, hardware security modules) used as a 'root of trust' or 'secure elements' for applications in passports, digital identity cards, smart meters, tachographs, smart phones, trusted platform modules etc (ii) cloud services; (iii) 5G.

In absence of harmonised rules, users, such as critical infrastructures obligated under the revised NIS Directive to take their supply chain security more seriously, may start putting in place diverging contractual requirements for manufacturers of products with digital elements.

At **global level**, it can be assumed that the security of supply chain measures taken recently, in particular in the United States of America (notably mandatory measures for critical software under public procurement) and the UK (notably security requirements of consumer IoT), as well as potentially further similar measures, would influence the playing field for European manufacturers present on global markets, potentially putting them at a disadvantage. A horizontal European regulation in this regard would be the most comprehensive to be introduced world-wide, creating legal certainty and getting Europe to set the path forward for cybersecurity in products with digital elements at global level.

As described in *section 2.4*, some problem drivers may diminish in the future. The labour market may for example provide more qualified security professionals, either as a result of market forces or due to government intervention. Awareness raising campaigns and adapted school curricula may also lead to users become more aware of cybersecurity risks and more proficient in using producta with digital elements securely. Additional international standards on products and processes may also emerge, helping manufacturers improve the design and development of products with digital elements.

5.2. Description of the policy options

The policy options analysed range from the least interventionist and closer to the baseline scenario (option 1 – soft law approach and voluntary measures), through a lighter option that could entail certain legislative interventions on a case-by-case basis (option 2 – ad-hoc regulatory intervention), up to the most interventionist (options 3 and 4 – horizontal regulation on cybersecurity), with option 4 varying in relation to scope (option 4 b) having the most comprehensive scope, all products with digital elements, covering also non-embedded software). Both policy options 3 and 4 also vary in relation to the level of conformity assessment (with and without mandatory third-party assessment). Furthermore, the various options analysed took account of the extent to which various measures, vertical or horizontal, or combination thereof could address the type of cybersecurity risks the products with digital elements are exposed to and the problems identified and their drivers.

Policy options 3 and 4 are based on the New Legislative Framework (NLF). The NLF places obligations on manufacturers and their authorised representatives as well as on importers and distributors. A detailed description of the NLF can be found in *Annex 11*. The NLF is primarily a framework placing obligations on economic operators, as the aforementioned types of entities. As a result, it is not foreseen to place obligations on users, such as consumers as well as companies or other types of organisations.

Departing from the status quo, the following options are therefore considered in view of the specific objectives to be achieved as set out in *section 4.2* above.

Option 1: Soft law approach and voluntary measures

In this option, there would be no mandatory regulatory intervention. Instead, the Commission would issue **communications, guidance, recommendations** and potentially **codes of conduct** to encourage **voluntary measures (self regulation)**, **including potentially on non-embedded software**, and **provide guidance** to support supply-side stakeholders to enhance the digital security of their products. These guidelines or recommendations could consider the elements that are referred to in options 3 and 4 below under the potential cybersecurity requirements. Such

recommendations or guidelines could also be limited only to the **public procurement** of products with digital elements,[127] given existing practices of public procurement which oftentimes include security-related considerations, such as due diligence in respect of cybersecurity when procuring certain products with digital elements in certain sectors or by certain agencies. Recommendations for public procurement may also ultimately have broader effects beyond strictly the public procurement framework and be also considered in private procurement a good practices.

At the same time, it would be expected for the Union Rolling Work Programme for European cybersecurity certification,[128] on the basis of Article 47(5) of the Cybersecurity Act, to consider the development of **additional European cybersecurity certification schemes** that would cover more categories of products for which cybersecurity is currently not being properly addressed, such as industrial IoT. These schemes would remain voluntary, unless otherwise decided via a delegated act for particular categories of products used in particular sectors through the empowerment provided to the Commission on the basis of the NIS2 Directive,[129] once it enters into force.

National schemes (e.g. labelling), voluntary or mandatory, would continue to be developed to compensate for the lack of EU horizontal rules.

Option 2: Ad-hoc regulatory intervention for cybersecurity of tangible products with digital elements and respective embedded software

This option would entail an ad-hoc product-specific regulatory intervention that would be limited to adding and/or amending the cybersecurity requirements in the already existing legislation or introducing new legislation as new risks emerge, including potentially on non-embedded software. A number of legislative initiatives or reviews are currently being prepared or negotiated with a view to integrate more broadly digitization and the development of new technologies, with a tendency to cover certain cybersecurity aspects, either through a safety angle (see the general product safety framework) or more specifically to certain technologies or products (e.g. AI). A scenario where this approach would be continued, in the absence of a horizontal intervention, can therefore be considered realistic.

More specifically,

i. **For existing NLF legislation**,[130] it would entail:

- case-by-case analyses that may lead to legislative amendments (*gradually or at once*) in relation to those products that have a digital element, but for which the existing legislation does not foresee any cybersecurity requirements.
- based on a case-by-case analysis, consider amendments to legislation already containing certain cybersecurity requirements, to the extent necessary, to include more specific or targeted cybersecurity requirements, including where applicable in relation to embedded software. This could a possible amendment of the RED Directive in order to equally extend the scope of the RED delegated act and to include non-embedded software as well as a duty of care obligation for the whole life cycle of the product.

[127] This is an approach taken, for example, by the US with regard to certain categories of products.
[128] Programme which aim is to identify strategic priorities for future European cybersecurity certification schemes, as provided for by Article 47 of the Cybersecurity Act. The programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.
[129] Article 21 of the NIS2 proposal.
[130] For more details relating to NLF legislation, see the explanations below under this section and *Annex 11.*

ii. **For future NLF legislation**, it would entail:

- cybersecurity requirements to be introduced when new product (NLF) legislation is developed and cybersecurity relevant.

iii. **For 'old approach' product legislation**,[131] it would entail:

- Where necessary and where the basic acts allows, introducing amendments, in particular for empowerments on complementing or further specifying cybersecurity requirements via delegated or implementing acts.

Note: *The **next two options (3 and 4)** entail a horizontal regulatory intervention varying in scope, largely following the **NLF approach**. This framework typically sets **essential requirements** as a condition for the placement of certain products on the internal market. These requirements are objective-oriented, followed at a later stage by harmonised standards developed by standardisation bodies, which elaborate on the technical means through which the requirements could be met. More information on standards can be found in Annex 14.*

*NLF legislation also typically provides for **conformity assessment**, which is the process conducted by the manufacturer to demonstrate whether the essential requirements relating to a product or process have been fulfilled. Conformity assessment procedures are composed of conformity assessment modules defined by the NLF, ranging from self-assessment by the manufacturer up to the assessment in certain circumstances, or in consideration of certain risks, by independent third parties. The latter are known generally as conformity assessment bodies, or more formally as 'notified bodies'. Member States have the responsibility to decide which of their conformity assessment bodies fulfil the necessary criteria to become notified. This may happen through an accreditation process. Accreditation is a formal system which provides an independent attestation of the competence, impartiality and integrity of conformity assessment bodies. The NLF framework also typically provides for EU **market surveillance**, which is under the responsibility of the Member States. For more details, see Annex 11.*

Option 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

This option would entail a **regulation introducing horizontal cybersecurity requirements for all tangible products with digital elements and the software embedded** within these, as a condition for placement on the market. Non-embedded software would not be regulated. Given its relatively broad scope and since the policy option proposes both security requirements as well as transparency requirements, policy option 3 addresses all four problem drivers as far as hardware products and their embedded software is concerned. Obligations would apply to manufacturers and to a lesser extent to also to distributors (such as online shops or brick and mortar stores) as well as to importers. The main building blocks of the regulatory intervention under this option would be as follows:

a) Scope:

[131] In the context of EU sector specific safety legislation, so-called old and new approaches are traditionally distinguished. The 'Old Approach' refers to the very initial phase of EU regulation on products, whose main feature was the inclusion of detailed technical requirements in the body of the legislation. Certain sectors such as food or transport are still being regulated on the basis of 'old approach' legislations with detailed product requirements. The so-called 'New Approach' was developed in 1985, whose main objective was to restrict the content of legislation to 'essential (high-level) requirements' leaving the technical details to European harmonised standards. On the basis of the New Approach, the New Legislative Framework (NLF) was then developed in 2008, introducing harmonised elements for conformity assessment, accreditation of conformity assessment bodies and market surveillance. Today more than 20 sectors are regulated at EU level based on the NLF approach, e.g. medical devices, toys, radio-equipment or electrical appliances.

- **all tangible products with digital elements, i.e. hardware** (e.g. *end devices* such as: laptops, smartphones, sensors and cameras; smart robots; smart cards; smart meters; mobile devices; smart speakers or *networks,* such as: routers; switches)
- the respective **embedded software associated with these products**, meaning firmware or other software that is essential for the function of the end-product (e.g. operating systems; network system; storage and security management, etc.).

It will not cover non-embedded software, meaning software that is additional to the function of the device on which it is downloaded (e.g. extended operating system, mobile apps). Instead, a **staggered approach** would be considered**,** with **soft law** measures such as guidelines or recommendations taken as a first step, potentially followed by horizontal regulatory intervention, depending on the results of implementing such measures. The reason is that traditionally non-embedded software is not covered by existing product legislation within the NLF and therefore an intermediary period could be considered via soft law measures to test the potential uptake by the relevant software manufacturers.

The rationale of analysing an option not covering non-embedded software in the scope is as follows: (i) it corresponds to the current NLF legislation, which covers as a rule tangible products and at most their embedded software and (ii) it is an option suggested by certain stakeholders on the grounds that more judicious consideration is necessary before imposing cybersecurity requirements on non-embedded software due to its intangible nature.

The definition of "product with digital elements" would specify that "products with digital elements" refer to both hardware and software as well as hardware and software components placed on the market separately.

b) Requirements and obligations:

In terms of **cybersecurity requirements and obligations for economic operators**, it would mandate that tangible products with digital elements and their embedded software shall only be made available on the market if, where dully supplied, properly installed, maintained and used for their intended purpose or under conditions which can be reasonably foreseen, they meet the specific cybersecurity requirements. While manufacturers would be required to comply with the requirements, they would not be held accountable for how the product will be used.

Nature of the requirements: These requirements would be **objective-oriented, technology-neutral and future proof** against a fast-evolving product and technology landscape. They would not be sector or product-specific. In terms of granularity, they would not be too prescriptive as they would be applicable to a wide category of products, yet more specific than a very generic principle that would only require that products are cyber secure or protected.

***Content of the requirements*:** The requirements would **mandate** manufacturers to factor in **cybersecurity in the design and development** of the products with digital elements, to exercise **due diligence** on security aspects when designing and developing their products, to be **transparent** on cybersecurity aspects that need to be made known to customers and to ensure security **support (updates)** in a proportionate way.

More specifically, manufacturers would mainly be mandated to:

- Design and develop these products in consideration of the risk posed to the security of network and information systems.
- Design and develop these products in such a way that they provide **adequate resilience against security threats,** ensure that the products can be **used securely** and ensure protection of stored, transmitted or otherwise processed **data** and that security is taken into account, as applicable, **in all phases** of the **design, development and production process**.

- Put in place design and development solutions for the product, i.e. **security by design and by default** mechanisms[132], to deliver with a secure by default configuration; capabilities to perform or support integrity checks; authentication and access control mechanisms;guarantees for protection of the exposed attack surfaces; protection against degradation or denial of service attacks; ways for enabling adequate security updates and ensure that adequate security support can be received.
- In addition to the product-related security requirements described above, have in place **vulnerability management, vulnerability disclosure policies and testing**.
- In addition, to ensure the effective functioning and security of the internal market and awareness of cybersecurity risks by relevant authorities and bodies, manufacturers should **report vulnerabilities** that are being actively exploited and any incident having an impact on the cybersecurity of these products to the EU agency for cybersecurity, ENISA. Based on the received information, ENISA should prepare intelligence on emerging trends regarding cybersecurity risks in products with digital elements to the national competent authorities and the European Commission, e.g. in the NIS Cooperation Group, as well as provide advice to support the implementation process of this Regulation.

These requirements derive from the overall objective of ensuring a high level of cybersecurity of products with digital elements. They take account of well-settled practices in terms of cybersecurity of products, factoring in the security objectives that the Cybersecurity Act establishes, as well as existing international standards for certain specific products[133], such as the ETSI standards for IoT consumer products.[134]

The above-mentioned requirements are inter-dependent and complementary to each other, ensuring as a whole that the respective product would be secure. For example, for certain risks and intended use cases it may be appropriate to integrate an authentication mechanism into a device to prevent unauthorised access and data theft (requirement "*protection from unauthorised access by appropriate control mechanisms*"). For this requirement to be effective, it is essential that other requirements are fulfilled as well: for instance, if the device is shipped with a widely-known default password, a malicious actor could access the data despite an adequate authentication mechanism being in place. The device should therefore not be shipped with any default password, but instead require users to select a strong custom password upon first use (requirement *"delivered with a secure by default configuration").*

In addition to the above-mentioned requirements concerning the products as such, obligations would be set up for economic operators, starting from manufacturers, up to distributors and importers, in relation to the placement on the market of the tangible products with digital elements and their embedded software, as adequate for their role and **responsibilities on the supply chain**. These obligations would mainly be:

- **Transparency-related**, including in terms of information made available to end users, keeping records or disclosure of information concerning the components of a product, ensuring **duty of care**, **vulnerability disclosure.**
- Making available **technical documentation**.
- Providing **information and guidance** to users on cybersecurity aspects.

Who should respect these obligations? When placing any product with digital elements on the market, manufacturers would be required to ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out by the regulation.

132

133 Such as IEC 62443 series

134 ETSI: "Consumer IoT security".

This would apply no matter whether the product is for end users or embedded in a final product. For tangible products with digital elements and software embedded in such products that is essential for the functions of these products, the responsibility for the compliance with the essential cybersecurity requirements would pertain to the manufacturer of the whole product.

The essential cybersecurity requirements would be followed by a **standardisation mandate** for the standardisation bodies to develop harmonised standards which would set out the technical specifications, some product or sector-specific, by which compliance with the requirements could be ensured.

The regulation setting out the horizontal requirements would not provide for liability rules. These are set out by the general EU product liability framework[135] (currently under review) which sets out liability rules for defective products so that consumers can claim compensation for damage caused by defective products. The Product Liability Directive establishes the principle that the manufacturer of a product is liable for damages caused by a defect in their product irrespective of fault ("strict liability"). It defines the conditions that allow injured parties to seek redress from injuries or damage to personal property caused by defective products marketed within the EU.

c) Whole life cycle:

As regards market placement coverage, the whole life cycle of the products with digital elements would be considered, and in particular obligations for manufacturers to provide **information** about the **end-of-life** of the products and **the security support provided,** as well as obligations to provide **security updates** and support for a **reasonable period of time** (e.g. average of five years), while ensuring proportionality.

This approach would be compatible with the EU **framework on liability for defective products**, now undergoing review, which, among others, aims to take into account the dynamics and seriousness of cybersecurity threats and which is expected to introduce liability for situations when damages are triggered by vulnerabilities. The liability of an economic operator may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person [including, for example, rejecting a software security update] or any person for whom the injured person is responsible.

In the absence of corresponding horizontal regulation setting out post-market placement security obligations on manufacturers, the leverage of the future product liability framework (currently under review) on the manufactures who may be held liable for damages caused by lack of cybersecurity measures would be more limited. For example, absent specific cybersecurity requirements that manufacturers must comply with in relation to their products with digital elements, there will be more limited ways to successfully trigger liability for damages caused by cybersecurity-related defects of such products.

d) Conformity assessment:

Different **sub-options** may be considered with regard to the **conformity assessment procedures**:

- **Sub-option 3 i)** No risk categorisation and self-assessment of conformity by manufacturer only, while manufacturers may voluntarily opt for a third-party conformity assessment when deemed appropriate.
- **Sub-option 3 ii)** Two risk categories:
  - by default: self-assessment, and

[135] Product Liability Directive: Directive 85/374/EEC.

- critical products: third-party conformity assessment prescribed for certain categories of products under a risk-based approach. The categories would be explicitly listed in the horizontal regulation, with the possibility to be updated based on a delegated act empowerment and could include, for example, products such as critical software, products that serve as safety components, industrial IoT and industrial control systems. They would take account of factors such as intended use or functionality :
  - ✓ *based on cybersecurity functionality,* software products that have *security-critical functions* or pose similar significant potential for harm if compromised;[136]
  - ✓ *based on intended or reasonably foreseeable use or potential risk of physical harm:* products with digital elements intended to be used in a sensitive environment, including in critical infrastructures or in an industrial setting.
- In addition, an empowerment for delegated acts would be considered for the Commission to specify, based on established criticality criteria in the basic act, the categories of products for which certification, on the basis of EU cybersecurity certification schemes established by the Cybersecurity Act would be required. See table in *Annex 12* illustrating the two-level risk categories for the conformity assessment.

Even if not mandatory, EU cybersecurity certification schemes would also continue to be used based on the Cybersecurity Act and, where applicable, could be used as evidence to demonstrate compliance with the essential requirements. It would rather be expected however for the planned new European cybersecurity certification schemes regarding products with digital elements to be more limited in this option than in the status quo or in option 1 or 2.

Where compliance of the product with the applicable essential requirements has been demonstrated, either via self-assessment modules or by a third party, manufacturers would draw up an EU declaration of conformity and affix the CE marking.

e) Interplay with other product-related legislation (notably NLF):

The horizontal cybersecurity requirements in this option would come to complement and co-exist with existing product-related legislation.

The horizontal cybersecurity rules would establish non-product-specific essential cybersecurity requirements that would be considered a baseline for all products with digital elements. If justified by the particularities of certain products and if the horizontal rules, and the harmonised standards to be developed on this basis, would not suffice, additional product-specific requirements could still be established by dedicated legislation.[137] Furthermore, for certain specific NLF legislation, such as the proposed Machinery Regulation,[138] where certain product-specific cybersecurity requirements are already covered for safety components, the horizontal

[136] i.e. software that has, or has direct dependencies upon, one or more components with at least one of these attributes: designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing resources; designed to control access to data or operational technology; performs a function critical to trust; operates outside of normal trust boundaries with privileged access.

[137] For example, as regards Electronic Health Records, the recently adopted proposal on the European Health Data Space (EHDS) will add to and complement the envisaged EU horizontal cybersecurity legislation. The EHDS will complement the horizontal legislation with product-specific requirements, adapted to the health sector specific needs (e.g. security requirements for European health records systems which provide more specific requirements specific to these systems in certain areas, such as access control).

[138] Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM/2021/202 final.

cybersecurity requirements could include provisions to stipulate that those particular requirements would take precedence.

Overall, the act setting out the horizontal cybersecurity requirements would set out a rule of *lex specialis,* specifying that where, for a certain category of products with digital elements, the cybersecurity risks addressed by the essential requirements are covered by other more specific requirements of other Union harmonisation legislation, these horizontal cybersecurity requirements shall not apply to those products to the extent that the specific Union legislation in question sufficiently covers such risks, achieving the same level of protection as the horizontal requirements. In some cases, where the Union legislation in question contains requirements adapted to the sector-specific needs, including on software and general obligations on manufacturers, covering the whole life cycle of products, as well as conformity assessment procedures, the act setting horizontal requirements could exclude those products from its scope. This could be the case for Union legislation regulating medical devices,[139] certified aeronautical equipment[140] or potentially motor vehicles.[141] Even in those cases, the horizontal requirements would still apply to certain components of those products and eventually ensure a high level of security of the supply chain.

The relationship of policy option 4 with existing vertical cybersecurity regulation. The example of cars.

UN Regulation No 155 requires manufacturers to take a number of product- and process-related cybersecurity measures that are very similar to the requirements in policy options 3 and 4. Amongst others, manufacturers must perform an exhaustive risk assessment (that considers interactions with any external systems) and protect the vehicle type against risks. Manufacturers must also put in place a Cybersecurity Management System (CSMS) covering the whole life cycle of the vehicle. The CSMS must manage dependencies that may exist with contracted suppliers, service providers or manufacturers' sub-organizations, ensuring security throughout the supply chain. Those suppliers are not directly covered by UN Regulation No 155 but would be subject to the horizontal requirements for hardware and software under policy option 4. Therefore, it will be easier for vehicle manufacturers to manage their dependencies, as the components would carry the CE marking probing compliance with cyber-security requirements.

Under UN Regulation No 155, the car manufacturer must also take measures to secure dedicated environments on the vehicle type for the storage and execution of aftermarket software (such as software media players) and perform testing to verify the effectiveness of the measures. Such aftermarket products are not covered by the UN Regulation, but would be covered by policy option 4. This would contribute to increasing the security of motor vehicles.

Of all NLF legislation, the **case of the RED Delegated Regulation** requires particular attention, because this delegated act covers three general essential cybersecurity-related requirements for a big category of tangible products with digital elements (wireless hardware products) that would be also covered by the horizontal cybersecurity requirements. More specifically, the relevant

[139] For example, the existing legislation on medical devices (MDR: Regulation (EU) 2017/745) contains requirements regarding devices, including on software and general obligations on manufacturers, covering the whole life cycle of products, as well as conformity assessment procedures.

[140] According to Article 77 of the Regulation (EU) 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency (EASA), EASA is the responsible authority for the certification of relevant aviation products, parts, non-installed equipment and equipment to control unmanned aircraft remotely. The same or similar considerations would be applicable also to aerodrome equipment (Article 79) and air traffic management and air navigation services ('ATM/ANS') equipment (Article 80). The cyber resilience aspects of all aviation products falling under Regulation 2018/1139 are already included under the relevant technical requirements and are systematically assessed by the Agency during the certification process.

[141] The EU legislation on motor vehicles (Regulation (EU) 2019/2144, https://eur-lex.europa.eu/eli/reg/2019/2144/oj and Delegated Regulation (EU) 2022/545 supplementing Regulation 2019/2144 https://eur-lex.europa.eu/eli/reg_del/2022/545) introduces certain cybersecurity requirements, including on software updates, requiring compliance with specific UN regulations on technical specifications and cybersecurity (*UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387].),* and providing for specific conformity assessment procedures.

RED Delegated Regulation establishes the following three essential requirements for inter-connected radio equipment: (i) ensure network protection; (ii) ensure safeguards for the protection of personal data and privacy, (iii) ensure protection from fraud. A standardisation mandate is now being prepared, with standards likely to be developed within 2-3 years. The RED Delegated Regulation shall apply from 30 months after its entry into force.

In this option, the horizontal cybersecurity requirements would be more specific and granular than the general requirements set out in the RED Delegated Regulation for all wireless products. The RED delegated act would then be implemented until the horizontal cybersecurity requirements would start applying. From that moment, the cybersecurity requirements of the RED Delegated Regulation would become obsolete. A less optimal alternative would be to consider that compliance with the horizontal cybersecurity requirements could be presumed compliance with the cybersecurity requirements of RED delegated act.

Furthermore, when preparing the standardisation request for the horizontal cybersecurity requirements, it must be ensured that the standardisation work done with the respective RED Delegated Regulation is preserved and complemented only where needed.

See *Annex 9* for a detailed overview of the interplay with product legislation.

Option 4: A horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of tangible and non-tangible products with digital elements, including non-embedded software.

This option differs from option 3 only as regards the scope, as it **would include non-embedded software** (critical or all) in the scope of a potential regulation. Some particular elements of the regulatory intervention may however be impacted differently as compared to option 3 as a result of the differences in scope, as highlighted below.

a) Scope:

All products with digital elements, including non-embedded (standalone) software would be covered.

Alternative **sub-options** could be considered regarding the categories of software to be covered:

> **Sub-option 4 a)** would cover only critical software: critical software, such as operating systems or web browsers, would be defined as the software which has security-critical functions or which poses similar significant potential for harm if compromised. In particular, any software that has direct software dependencies[142] upon one or more components with at least one of these attributes: (i) is designed to run with elevated privilege or manage privileges; (ii) has direct or privileged access to networking or computing resources; (iii) is designed to control access to data or operational technologies; (iv) performs a function critical to trust;[143] (v) operates outside of normal trust boundaries with privileged access. Critical software as defined above is estimated at approximately 10% out of total software market. Furthermore, cybersecurity measures for critical software were also implemented in the Unites States of America, where the mandatory cybersecurity measures imposed concerned only critical software subject to public procurement, all other measures remaining voluntary (see *Annex 6*).
>
> **Sub-option 4 b)** all software: This would reflect the fact that all types of software products contain vulnerabilities and that even software considered as low risk can serve as a stepping stone to breach a network with a view to penetrating more critical systems at a

[142] For a given component or product, other software components (e.g., libraries, packages, modules) that are directly integrated into, and necessary for operation of, the software instance in question.
[143] Categories of software used for security functions such as network control, endpoint security, and network protection.

later stage of an attack chain. In addition, it is often difficult to assess the risk associated with a product before its placing on the market, as the risk to society often increased with a growing market share.

b) Requirements and obligations:

Horizontal essential cybersecurity **requirements** and corresponding obligations for operators as described above in option 3, including reporting of exploited vulnerabilities and cybersecurity incidents to ENISA, would be set out for all products with digital elements, including non-embedded software. For user-installed software [operating systems – except when the operator system is developed by the device manufacturer – and applications] and in general for non-embedded software, the responsibility for the compliance with the essential requirements would pertain to the software manufacturer.

c) Whole life cycle:

As regards market placement coverage, as in option 3, duty of care for **whole life cycle** would be provided for. This option would be even more fine-tuned than option 3 with the upcoming new EU framework for liability for defective products, considering that the latter also aims to extend liability explicitly for software.

d) Conformity assessment:

The same two **sub-options** as in option 3 would be considered with regard to the **conformity assessment procedures,**[144] corresponding respectively to **sub-options 4 a) i)** no risk categorisation, **4 a) ii)** with risk categorisation, **4 b) i**) no risk categorisation, and **4 b) ii)** with risk categorisation.

e) Interplay with other product-related legislation (notably NLF):

The interplay would be the same as set out in option 3 above *(see also for more details Annex 8)*. On the specific interplay with the RED Delegated Regulation, *Annex 7* illustrates the particular differences between the two acts. In this option, the horizontal cybersecurity requirements would address even more than in option 3 the existing gaps in what the RED delegated act covers, since they would also address standalone software.

In this option, the planning of future European cybersecurity certification schemes would be more impacted than in option 3, considering that, due to the comprehensive scope, there would be much less regulatory gaps to fill in with certification in addition to what the horizontal requirements would require. However, new European cybersecurity certification schemes could emerge for products with digital elements requiring additional assurance.

How would the horizontal cybersecurity requirements set for the broadest scope in option 4 work in practice? The example of smart phones.

Smart phones would be included in the scope of the horizontal regulation (policy options 3 and 4), as they are connected hardware devices with a built-in computational logic. Under policy option 4, manufacturers of such devices would be required to implement security requirements, undergo a conformity assessment and affix the CE marking.

A smart phone consists of a large number of hardware components, such as CPUs, wireless modems, Wi-Fi chipsets or Bluetooth interfaces, which the manufacturer must acquire from other semiconductor manufacturers. Furthermore, these hardware components function thanks to firmware (i.e. embedded software that provides low-level control of the components). Therefore, in addition to the manufacturer of the smart phone, the manufacturers

[144] Even in the case of sub-option 1.i. as regards the scope (i.e. only critical software), both sub-options could be considered, with the specification that in the sub-option entailing two levels of risks the critical software would be by default required to be subjected to third party conformity assessment, with potentially a sub-category thereof subjected to certification by national authorities.

of these hardware components and the software manufacturers of the firmware would also be covered under the scope of a horizontal regulatory intervention (both under policy option 3 and 4).

Smart phones are also usually shipped with an operating system (non-embedded software). The smartphone manufacturer would also need to ensure the security of the operating system. In cases where the manufacturer is also the manufacturer of the operating system, the security requirements that the manufacturer is required to implement would not only cover the hardware device, but would also extend to the software.

In cases where the operating system is provided by a third party, the manufacturer would need to check the CE marking affixed to the operating system to make sure that it has been developed in line with the requirements. The manufacturer of the operating system would equally be subject to such an obligation in relation to the various software components integrated during development.

Consumers and business users, and in particular companies that are subject to supply chain security obligations could rely on the CE marking as an indicator that not only the manufacturer of the final product has taken cybersecurity seriously during the development process, but also that all hardware and software components inside the product have been developed factoring-in security.

5.3. Options discarded at an early stage

In addition to the four options presented in *section 5.2,* in the analysis of potential policy options that could address the problems described in *section 2* and reach the general and specific objectives set out in *section 4*, a number of options or sub-options, notably in relation to alternatives entailing regulatory interventions, were discarded at an early stage and therefore not assessed in further detail, as follows:

(a). As regards the **choice of legal instrument**, the options consisting of a regulatory intervention (notably options 3 and 4) would entail the adoption of **a regulation and not a directive**. This is because, for this particular type of product legislation, a regulation would more effectively address the problems identified in *section 2* and meet the objectives formulated in *section 4*, since it is an intervention that is conditioning the placing on the internal market of a very wide category of products. The transposition process in the case of a directive for such intervention could leave too much room for discretion at national level, potentially leading to lack of uniformity of certain cybersecurity requirements, legal uncertainty, further fragmentation or even discriminatory situations cross-border, even more taking account of the fact that the products covered could be of multiple purpose or use and that manufacturers can produce multiple categories of such products.

(b). As regards the **scope of potential regulatory interventions in options 3 and 4**: Excluding the wireless products covered by the RED delegated act from the scope of the regulatory interventions envisaged in options 3 and 4 was not considered a valid sub-option. This is because the essential requirements set out in the RED delegated act are of generic nature, while covering a wide category of products (inter-connected radio equipment) that represent an important part of the overall scope considered for the horizontal cybersecurity regulatory intervention in options 3 and 4. The essential requirements in the RED delegated act alone would not sufficiently address the problems identified, as described in *section 2*, nor would they be sufficient to effectively meet the objectives set out in *section 4*. Furthermore, aspects such as duty of care or whole life cycle are not covered by the RED delegated act. Before new horizontal cybersecurity rules would start applying, important progress would have been achieved with the implementation of the RED delegated act, including preparation of standards, which would also take account of the proposal for a horizontal regulation. A smooth sequencing between the two acts would then be ensured, without generating overlapping or unnecessary burden on the relevant economic operators concerned by such obligations.

(c). In relation to the horizontal cybersecurity requirements envisaged in options 3 and 4, the sub-option of **differentiating such requirements per category of risks** was discarded at an early stage. This is because such sub-option would have been unrealistic, given that the

requirements would in any case be objective-oriented and aim at setting basic requirements for introducing security by design and by default, ensuring transparency, duty of care throughout whole life cycle. These would be baseline requirements that all products with digital elements should have in place irrespective of their functionalities or intended use. The differentiation per categories of risk would rather have relevance for informing the strictness with which compliance with the requirements is assessed. It can only be reflected in more sector- or product-specific standards.

(d). As regards still the horizontal cybersecurity requirements envisaged in options 3 and 4, the sub-option of **differentiating such requirements between Business to Client (B2C) and Business to Business (B2B)** was discarded at an early stage. This is because essential cybersecurity requirements as those that would be set out through a horizontal regulatory intervention would be objective-oriented, hence the same irrespective of the use case, with the aim to ensure that security is factored in since the design and the development of the respective products. These would therefore not differ depending on the user. Furthermore, many products with digital elements are used in both settings.

(e). As regards the **duty of care throughout the life cycle** of products with digital elements, the potential legislative interventions analysed did not consider the alternative of not covering whole life cycle at all as a valid option. This type of coverage is coherent with other current legislative reviews considered, such as the EU product liability framework, and is also determined by the very nature of the requirements considered, i.e. in cybersecurity the updates are a necessity, therefore any alternative where no obligation concerning the life cycle would have been considered would not have been realistic. Furthermore, the coverage of whole life cycle is one of the aspects regarding a horizontal cybersecurity intervention for products with digital elements where the vast majority of stakeholders concur.[145]

(f). As regards market surveillance, policy options 2, 3 and 4 would plug into the New Legislative Framework. Market surveillance would therefore be based on an existing and well-established concept. As a result, governance rules for market surveillance authorities going beyond the standard NLF provisions leaving discretion to Member States on how they organise themselves was not considered as a realistic option for a first-time market intervention of this breadth.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

6.1. Overview of impacts on businesses, public authorities and consumers

To the extent possible, specific and aggregated quantitative estimates have been elaborated for the different sources of costs and benefits. However, the ability to develop such quantitative estimates was limited by different factors, such as the multitude of specific product markets covered by the initiative and the ability to define at granular level the markets in the scope of the different policy options. Where possible, estimates and assumptions were made. Different methodologies were used for the quantification of costs and benefits that will be indicated in the relevant sections. Furthermore, the quantitative analysis of costs and benefits uses in a consistent way for the aggregation several key assumptions that are further explained in *Annex 4*:

- **Estimation of number of products**: To estimate the number of products with digital elements on the market, the assumption of one product per manufacturer was used. The indicator extended classification (ICT-EXT-ADJ, see *section 5.1.* and *Annex 3*) for hardware was used. Combined with the indicator for software (SD), **615 272 manufacturers/products** are counted on a market that is valued in total at up to EUR 1

[145] 90 % of the participants to the public consultation believe that hardware and software manufacturers should be responsible for the full life cycle of a product with digital elements (such as by providing updates), including 79 % of SME manufacturers.

485 billion in turnover[146]. While it is an underestimation to count one product with digital elements per manufacturer, as large companies might develop hundreds of products, it is compensated to some extent by the choice of using a broad indicator for the hardware market. Furthermore, the aggragted estimations have been made based on the assumption that all products currently on the market would be impacted, while under policy option 3 and 4, costs would actually occur for new products being placed on the market.

- **Business as usual (BaU)**: based on available data, it is estimated that 50% of manufacturers have a systematic approach to secure product development, while for the rest, it is assumed that they have no security requirements in place. For conformity assessment, the BaU costs are estimated at 40% for hardware manufacturers, and at 25% for software manufacturers. For further background, see *Annex 4*.
- **Average product development costs**: it is estimated that on average development costs by product are of 140 000 EUR. For further background, see *Annex 4*.

For the qualitative assessments of impacts, in order to compare the policy options (and sub-options), a scale from *Neutral* to +++ has been used (with "+++" indicating the highest impact).

The table below presents an overview of the main (direct and indirect) economic, internal market, security, competitiveness, social, environmental and fundamental rights impacts and stakeholders affected that will be analysed more in detail in the following sections for each policy option.

	Affected stakeholder	**Main impacts**	
		Costs	**Benefits** (Direct and indirect)
Businesses	Software & hardware manufactures	— Direct compliance costs (e.g. security requirements; information obligations; documentation; testing; reporting obligations)	— Streamlined requirements for products with digital elements — Reduced cyber incidents (costs of reputation) — Higher uptake of products with digital elements in and outside the EU (turnover)
	Importers of products with digital elements	— Direct compliance costs (familiarisation; verification)	— Higher uptake of products with digital elements in and outside the EU (turnover) — Reduced cyber incidents (costs of reputation)
	Distributers of products with digital elements	— Direct compliance costs (familiarisation; verification)	— Higher uptake of products with digital elements in and outside the EU (turnover) — Reduced cyber incidents (costs of reputation)
	Businesses as end-users	— Higher prices of products with digital elements	— Higher transparency on security properties and on secure use of products with digital elements — Reduced cyber incidents (costs of handling & reputation) — Reduced cyber mitigation costs — Reduced compliance costs to meet other EU and national cyber legislation (e.g. NIS)
	Notified bodies	— Direct compliance costs (e.g. training and new staff; accreditation framework)	— Increased turnover — Streamlined requirements for accreditation related to security of products with digital elements
Public authorities	Market surveillance authorities (MSAs)	— Direct compliance costs (e.g. training and new staff) — Enforcement costs (e.g. monitoring and inspection)	— Overall benefit of public interest of ensuring that products with digital elements accessing the internal market are secure — Cost savings due to streamlined requirements for market surveillance of products with digital elements
	Accreditation and notifying authorities	— Direct compliance costs (e.g. training and new staff) — Enforcement costs (monitoring)	— Streamlined accreditation and notification requirements — Fees from notified bodies

[146] The methodology for the market indicators is further explained in Annex 3.

	Public authorities as end-users	— Direct compliance costs (e.g. familiarization for public procurement) — Higher prices of products with digital elements	— Transparency on security properties and on secure use of products with digital elements — Reduced cyber incidents (costs of handling & reputation) — Reduced cyber mitigation costs — Reduced compliance costs to meet other EU and national cyber relevant legislation (e.g. NIS)
	ENISA	— Direct compliance costs (collect and disseminate information on exploited vulnerabilities)	— Enhanced transparency on the security of products with digital elements
Consumers and citizens	Consumers and citizens	— Higher prices	— Transparency on security properties and secure use of products with digital elements — Enhanced protection of fundamental rights, especially privacy and data protection (reduced data breaches)

Table 2: Main impacts and stakeholders affected

6.2. Economic impacts

This section analyses economic impacts on businesses, SMEs, public authorities and users.

6.3.1. Impacts on manufacturers of products with digital elements and other economic operators

The impacts in terms of costs and benefits on businesses, including manufacturers, distributors and importers, will stem from, on the one side, compliance costs, and on the other side, increased reduced cyber incidents, reputation, competitiveness and increased uptake of products with digital elements. The impact on SMEs, including as economic operators, is detailed in section *6.3.2*.

Analysis of compliance costs

Direct compliance costs will impact most significantly software and hardware manufacturers. The overview of the main cost sources is summarised below:

a) **Familiarisation** with the new obligations (one-off): manufacturers, distributors and importers covered by the initiative will have to bear adjustment costs to familiarise with the obligations under the new legislation and develop compliance strategies (implementation costs).
b) **Secure product development throughout the life cycle** (one-off and recurrent), including requirements related to vulnerability handling as well as support and security updates: Adjustment costs would stem from the implementation of security controls and features into the product design and development (one-off and recurrent for checking regularly compliance and implementing updates), hiring skilled human resources, and from potential equipment and material costs (e.g. new security software). Security controls and features would also include obligations to communicate and inform end users on the lifespan of the product and provide security support.
c) **Information and transparency requirements** to end-users on secure product properties and instructions for use (one-off and recurrent): Adjustment costs would stem from information obligations on the security properties and use of the digital product.
d) **Conformity assessment:** internal product testing/self-assessment, one-off costs, e.g. for the purchase of laboratory and testing equipment for internal testing, and recurrent costs, e.g. for the recalibration of testing equipment and reporting, as well as third-party product testing and certification (one-off for the certification fees and recurrent for maintenance of the certification, e.g. regular audits). For more background on testing costs, see *Box 2*.
e) **Other conformity costs and reporting obligations:** companies will need to develop a technical documentation and a declaration of conformity, affixing marking on products and report on the conformity of products at the request of authorities as well as reporting of

exploited vulnerabilities and incidents to ENISA. Internal systems and procedures need to be put in place to ensure that the technical documents and declaration of conformity are updated regularly. Furthermore, vulnerability and incident reporting requirements will represent both one-off and recurrent costs for businesses (e.g. to set up the reporting systems and to report regularly on events).

Quantitative estimates are provided to the extent possible, and mostly available for policy options 3 and 4. Due to the limited data available, the provided estimates only represent average and abstract figures. It could not be distinguished between one-off and recurrent costs. In general, as highlighted by stakeholders,[147] the **compliance costs for a company will greatly vary depending on: (i) the complexity and size of the product; (ii) the existing security practices of a given company; (iii) the environment (B2C vs. B2B), and (iv) the size of the company.**

Unless specified, the quantitative estimates express additional compliance costs, taking into account the Business as Usual (BaU) costs. BaU costs capture existing costs in the absence of any policy measure. *Box 1* summarizes the methodological steps, assumptions and limitations.

Summary and limitations of methodological approach on quantification of compliance costs

In order to estimate the direct compliance costs for businesses, the following steps have been taken:

1. *First, the relevant stakeholders that would be impacted by direct compliance costs have been identified. This includes economic operators subject to direct obligations, i.e. manufacturers (of software and hardware), distributors and importers.*
2. *The different cost sources that would affect the economic operators were identified and verified through stakeholder consultations, including the public consultation and targeted workshops and surveys (see Annex 2).*
3. *For each cost source, estimates on the product development costs were gathered from **primary and secondary sources**. The data that could be gathered is limited. Only one primary source estimation was used for the cost source related to documentation and reporting under policy option 3 and 4, however this cost estimation could not be verified. Secondary data was used for major cost estimates, such as conformity assessment and secure product development. No cost estimates could be made for a number of costs sources, such as familiarisation with the requirement of the initiative and providing information to users.*
4. *Where data could be found, **average cost estimates for an abstract product unit** were made. On this basis, the costs were aggregated for the market in the scope of the relevant policy option. The Standard Cost Model could not be applied due to limited data available.*
5. *In order to **aggregate the costs**, the **number of products with digital elements** that would be impacted was estimated, taking into account a general assumption of BaU costs, and multiplying by the average product unit costs. The main product markets were identified, respectively the software and hardware market, based on the ICT-EXT-ADJ and SD market indicators (see Section 5.1. and Annex 3), and the scope of the relevant policy options were delineated to the extent possible. In some cases (e.g. for critical software), assumptions for the market share had to be done due to a lack of granularity of market data. In order to apply the BaU costs, assumptions have been made on the percentage of businesses already implementing the relevant measures, as detailed in Annex 4.*

Box 1: Overview of methodological steps for the quantitative analysis of compliance costs

Policy option 1

Given that the measures will be voluntary, under this option only the participating **manufacturers** would bear possible additional adjustment and administrative costs. As these costs would depend on the engagement of the manufacturers into voluntary initiatives, it is not possible to give aggregated cost estimates. Under policy option 1, there would be no direct compliance costs on **importers** and **distributors.**

[147] Stakeholder workshop of 10 May 2022 organised by the study supporting this impact assessment, see *Annex 2*.

Adjustment costs for manufacturers would stem from implementing security requirements as foreseen in relevant guidelines or recommendations. To estimate the costs of secure product development, secondary data was used, which is the Venson calibration model (further developed in *Annex 4*). According to this academic research, implementing a secure product development life cycle approach, without any requirements in place, would on average add 30.5% of product development costs (if no comprehensive security measures are in place). **Administrative costs** would be linked to third-party conformity assessment procedures to be carried out under voluntary EU certification schemes, and could range between EUR 25 000 to 40 000 per product, according to secondary data[148].

The economic cost impact of option 1 is likely to be low on manufacturers, and neutral on distributors and importers. The BaU costs are expected to be high as the manufacturers participating to voluntary initiatives are likely to be the more security-minded. Furthermore, it can be assumed that those manufacturers participating in such voluntary measures would expect any additional costs to be offset by direct or indirect benefits (e.g. increase their reputation and market share).

For this policy option, stakeholders indicated in the public consultation **low to medium costs** (on average 2.5, with 5 being the highest) with the highest average costs for the compliance with guidelines on public procurement.[149] For communications, guidance and recommendations, stakeholders indicated on average the cost would be medium[150]. The use of voluntary European cybersecurity certification, on the basis of the Cybersecurity Act, was rated as **high** by software and hardware manufacturers.[151] Despite being voluntary, business representatives stressed that certification involves costs when it is required by customers. At the same time, the possibility to obtain an EU wide certificate would reduce costs for those manufacturers that already certify their products or would act as an incentive for those willing to do so.[152] Such certification costs would in any case occur in the status quo as well, therefore the BaU costs would be high.

	Costs (administrative and adjustment costs)
Commission (voluntary) recommendations and guidance	• Secure product development costs for those manufacturers that decide to apply the measures = +30.5% of product development costs if no BaU costs, on average EUR 42 700 for a product unit cost of EUR 140 000. • No costs for importers and distributors
Additional (voluntary) EU certification schemes	• Compliance costs for manufacturers that engage in EU certification (ca. EUR 25 000 to 40 000 for certifying a product[153]) • No costs for distributors and importers
Total	*Neutral/+*

Table 3: Overview of compliance costs on businesses under policy option 1

Policy option 2

Under this policy option, direct compliance costs for hardware and software manufacturers (for embedded and possibly non-embedded software), as well as distributors and importers would stem mainly from the amendment and addition of cybersecurity requirements in already existing and future NLF legislation. Such amendments would address new risks as they emerge, including potentially for non-embedded software.

[148] SWD(2017) 500 final, IA accompanying the Cybersecurity Act, based the costs of national cybersecurity certifications
[149] The costs were estimated to 2.97 in average, with hardware manufacturers rating it 2.9 and software manufacturers 2.83.
[150] rated the costs at 2.54 out of 5 (with 5=very costly). Software manufacturers indicated a slightly higher cost (2.69) compared to hardware manufacturers (2.2).
[151] 3.05 and 3.31 out of 5 respectively for hardware and software manufacturers.
[152] See also SWD(2017) 500 final, IA accompanying the Cybersecurity Act.
[153] SWD(2017) 500 final, IA accompanying the Cybersecurity Act, based the costs of national certifications

When asked in the public consultation, stakeholders rated on average the costs of this option as **medium to high** with 3.36 out of 5 (with 5 indicating very high costs). Hardware manufacturers rated the costs related to this option higher than software manufacturers (4.06 vs. 3.73 out of 5).

In relation to compliance costs, two main situations can be distinguished, depending on whether non-embedded software is brought into the scope through amending an NLF legislation or not.

- If only hardware manufacturers and manufacturers of embedded software would be concerned, the BaU costs for hardware manufacturers are expected to be high. The amendment of existing NLF legislation would imply, for a given product, adjustment costs related to the familiarisation and additional security and information requirements linked to the lifecycle approach and increased transparency. Option 2 foresees no specific conformity rules for cybersecurity requirements only. Therefore, minimal extra administrative costs would be foreseen (e.g. mainly updating technical documentation and the declaration of conformity). Since it would be determined on a case-by-case basis whether amendments are necessary, it was not possible to make general quantitative cost estimations.
- If non-embedded software manufacturers are to be covered by any amendment of existing or future NLF legislation, those manufacturers would bear high compliance costs. The aggregated costs would depend on the specific sector and the market share of such software.

- **Possible amendment of RED delegated act/Directive to include non-embedded software:**

As outlined in the baseline scenario in *Section 5*, if the RED delegated act would be amended to cover non-embedded software, additional adjustment and administrative costs would occur only to a limited extent for hardware manufacturers already subject to the RED delegated act (i.e. mainly related to lifecycle approach) and would mostly occur for non-embedded software manufacturers. Furthermore, distributors and importers would bear additional familiarisation costs. The cost estimation will focus on the costs on manufacturers of non-embedded software into the scope of the RED delegated act.

Based on the market analysis data available (see *Annex* 3), the assumption was made that all non-embedded software would be covered by this measure. To estimate the **adjustment costs** of secure product development, secondary data was used, which is the Venson calibration model that foresees 30.5% additional product development costs if nothing is in place (further explained in *Annex 4*). This leads to 42 700 EUR additional costs for a product unit when considering an average product development cost of EUR 140 000[154]. Furthermore, the assumption was made that 50% of software manufacturers already implement secure requirements (further explained in *Annex 4*). Taking the SD indicator (see market analysis in *Section 5* and *Annex 3*), and assuming one product per software company, the **software secure development costs** would amount to **EUR 7.8 billion[155]**. While this figure is likely an underestimation for the whole software market (as there are likely more software products), it goes beyond the scope of the measure (which would cover only wireless products).

Software manufacturers would also bear new adjustment and administrative costs related to conformity assessment (self-assessment) and other obligations linked to conformity. Secondary data was used to estimate the average costs for self-assessment, which is EUR 18 400 per self-tested product (2 staff per month)[156]. Taking the same market scope, and assuming that 25% of

[154] This assumption is further explained in Annex 4.
[155] 50% of 365 759 products, multiplied by 42 700
[156]Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report

the software manufacturers would already apply a similar form of testing[157], additional testing costs would amount to **EUR 5.1 billion**. Other conformity obligations (technical documentation, CE marking, declaration of conformity and reporting of exploited vulnerabilities and cyber incidents) would amount to **EUR 4.6 billion**, using a primary estimate of 9% average additional product development costs that could however not be verified[158]. Hence, the total aggregated compliance costs for software manufacturers would amount to **EUR 17.5 billion.**

	Costs (administrative and adjustment costs)
Amending security requirements in sectoral NLF legislation	*Depending on the sector where the legislation is amended* • For manufacturers: - Adjustments costs for secure product development (on average 30.5% if no BaU) - Familiarisation costs and updating technical documentation and conformity documentation • For importers and distributors: familiarisation costs
Bringing non-embedded SW into the scope of some NLF legislation and potentially duty of care for whole life cycle (e.g. RED DA)	• For manufacturers: - For software: **total compliance costs of EUR 17.5 billion** (not including familiarisation and information obligations) - Limited adjustment and familiarisation costs for hardware manufacturers • For importers and distributors: familiarisation costs
Total	+/++

Table 4: Overview of compliance costs on businesses under policy option 2

Policy option 3

Under policy option 3, compliance costs, both adjustment and administrative costs, would occur for all hardware manufacturers and embedded software manufacturers, as well as importers and distributors, due to the horizontal security requirements, associated conformity assessment and documentation and reporting requirements. The main costs for importers and distributors would be adjustment costs related to familiarisation related to the new requirements.

The impacts of policy option 3 will depend on the sub-options related to conformity assessment, respectively in sub-option 3 i) and 3 ii). In a first stage, only voluntary measures would apply to non-embedded software ("staggered approach). These cost impacts are described under option 1, and are not possible to be quantified. Furthermore, due to the lack of granularity of the market analysis, the aggregated impact on embedded software could not be estimated precisely.

In the public consultation, stakeholders rated the costs of "*Introducing mandatory horizontal cybersecurity requirements for hardware products"* on average at **medium to high**, with 3.55 out of 5 (with 5 indicating very costly).

Regarding **adjustment costs**, the main cost source will be related to secure product development. To estimate these adjustment costs, secondary data was used, which is the Venson calibration model that estimates an average of 30.5% additional product development costs if no security is in place (further explained in *Annex 4*). This leads to 42 700 EUR of additional product development costs for an average product with digital elements unit (EUR 140 000). Taking the assumption that 50% of hardware manufacturers are already implementing adequate security requirements (further explained in *Annex 4*), and estimating the number of hardware products impacted by using the ICT-EXT-ADJ indicator, the **aggregated additional costs** related to secure product development would be of EUR **5.33 billion**[159].

[157] The assumption of 25% is further explained in *Annex 4*.
[158] Targeted survey on impacts launched on 16 May 2022 organised by the study supporting this impact assessment. This estimate is likely leading to an overestimation as it brings the conformity costs close to the costs of testing. However, no other estimate could be found in primary and secondary data, and it was suitable to take into account these costs to estimate the administrative costs.
[159] 50% of 249 513 hardware products (based on ICT-EXT-ADJ), multiplied by 42 700 EUR

Adjustment costs related to **familiarisation costs** and costs related to **transparency and information** could not be estimated due to a lack of available primary and secondary data. For instance, in the case of the Toy Safety Directive, for importers, the time spent to comply with the Directive's requirements equalled to 110 man-hours per toy type (EUR 2 500). For distributors, time spent to comply with the Directive's requirements: 86 man-hours per toy type (EUR 1 953).[160] According to the targeted survey[161], the costs related to information and transparency would not be significant if provided in digital format.

Regarding **conformity assessment costs**, they are expected to vary depending on the sub-options related to conformity assessment. The average costs of conformity assessment per product with digital elements was drawn from secondary data. For self-assessment, the average cost was estimated at EUR 18 400 including one-off and recurrent costs (see *Box 2*). For third-party assessment, costs were estimated at EUR 25 000, which represents an average of possible costs for different types of products based on secondary data. *Box 2* further discusses the costs of self-assessment and third-party assessment. Costs related to conformity assessment would be both adjustment costs in the case of self-assessment (e.g. setting up and maintaining testing facilities) as well as administrative costs linked to certification fees paid to notified bodies to carry out audits and review documentation.

Under both sub-options **3i)** and **3ii)**, the **BaU costs** for conformity assessment for hardware manufacturers have been assumed to be on average at 40% both for self-testing and third-party assessment. This figure represents a low average of BaU cost evidenced. In the context of the Impact Assessment of the RED delegated act[162], the BaU for hardware products varied between 30 % for more simple products to 90 % for complex products such as routers. No data could be found on BaU costs for internal testing. These assumptions and estimates have **several limitations**:

- In the case of self-assessment (policy option 3i)), for hardware manufacturers already covered by NLF legislation (in particular RED), the BaU would likely be higher, as they could either follow the existing approaches on conformity assessment. The additional costs would mainly apply to non-wired hardware products on the market, of which the precise share could not be estimated[163]. Some of these manufacturers of non-wired hardware would likely also have internal testing practices in place.
- The BaU costs and additional testing costs would in practice greatly vary depending on the complexity of the product, as evidenced by the Impact assessment of the RED delegated act[164]. The costs increase with the complexity of the product, therefore it can be assumed that consumer products would generally bear lower costs for testing compared to industrial products. The BaU costs might be equally lower in the B2C compared to B2B sector, the latter being typically bound by more detailed contractual responsibilities. Therefore, the additional costs related to conformity assessment are expected to be higher on consumer products higher than for business products (for examples, see *Box 2*)**.**

Under **sub-option 3i)**, taking into account the BaU factor of 40% and the number of products based on the ICT-ADJ-EXT market indicator, and counting on average EUR 18 400 of internal testing by product, the aggregated additional costs related to the conformity assessment for the hardware market are estimated at **EUR 2.8 billion[165]**. Under **sub-option 3ii)**, taking into account the same BaU factor and market indicator, and the average costs of EUR 25 000 for third party

[160] Evaluation of NLF Regulation (2021)
[161] Targeted survey on impacts launched on 16 May 2022 organised by the study supporting this impact assessment

[162] See *Annex 4*, and SWD(2021) 302 final, IA supporting the RED delegated act
[163] This could include for instance wired IoT devices or computer components, including chipsets, memory chips or processors.
[164] SWD(2021) 302 final, IA supporting the RED delegated act
[165] 60% of 249 513 products, multiplied by EUR 18 400

assessment and assumig that the share of critical products should be narrow (ca. 10% of the market), the aggregated additional costs related to the conformity assessment for the hardware market are estimated at **EUR 2.9 billion**[166].

Other costs related to conformity, such as the technical documentation, the declaration of conformity, affixing of the CE market and reporting of exploited vulnerabilities and cybersecurity incidents to ENISA, have been estimated (using the estimate of additional 9% of product development costs based on primary data[167]) at **EUR 3.1 billion** for the hardware market.

As a result, in total, under policy **option 3 sub-option i)**, the total additional aggregated compliance costs (adjustment and administrative) would be of **EUR 11.2 billion**. Under policy **option 3 sub-option ii)**, additional aggregated compliance (adjustment and administrative) costs would be of **EUR 11.3 billion.** These figures do not include the costs for embedded software manufacturers, and therefore might be an underestimation.

	Testing costs	Other conformity costs	**Total conformity costs** (adjustment and administrative costs)	**Adjustment costs for secure product development**	**Total compliance costs**
3(i) self-assessment	EUR 2.8 bn	EUR 3.1 bn	EUR 5.9 bn	EUR 5.3 bn	EUR 11.2 bn
3ii) third-party assessment	EUR 2.9 bn - EUR 2.5. bn (self-assessment) - EUR 0.4 bn EUR (third-party assessment)	EUR 3.1 bn	EUR 6 bn	EUR 5.3 bn	EUR 11.3 bn
Voluntary approach on SW	See PO1				

Table 5: Overview of aggregated compliance costs on businesses under policy option 3.

Both under policy option 3 and 4, an important source of compliance costs would stem from the conformity assessment. Depending on the sub-options, third-party assessment would be foreseen for a narrow share of the market. Self-assessment (or internal testing) is generally seen as less costly than third-party assessment as it does not involve any notified body. However, the stakeholder consultations did not enable to make precise cost estimates to reflect the difference between the two assessment procedures. Business stakeholders generally stressed the importance for the manufacturer to have **flexibility** regarding the procedure.

Self-assessment of a product with digital elements typically includes (i) setting up an internal testing laboratory (one-off adjustment cost, e.g. train and hire staff); (ii) internal testing of a product with digital elements (recurrent). **Third party assessment** of a product with digital elements includes: i) the review of the technical documentation by a notified body; and ii) the testing and audit of the technical characteristics of the product with digital elements itself.

Throughout the consultations, stakeholders expressed different opinions as to whether self-assessment would be more or less costly compared to third-party assessment. During a consultation workshop,[168] most respondents said that the impact on costs of internal product testing/self-assessment would be "Low", followed by "Medium".

[166] 60% of 249 513 products, with 10% doing third-party assessment (average costs of EUR 25 000)
[167] Targeted survey on impacts launched on 16 May 2022 organised by the study supporting this impact assessment
[168] Stakeholder workshop of 10 May 2022 organised by the study supporting this impact assessment, see *Annex 2*.

Some stakeholders stressed that the costs will be less than third-party conformity assessment, and could be easily integrated in the internal product development process.[169]

During the same workshop, according to stakeholders, the impact on costs of external third-party product testing (or certification) would be **"**High", followed by "Very high". On the contrary, during the targeted survey,[170] interviewees stressed that one-off costs for self-assessment testing are quite high as it demands building internal capabilities, which could be cumbersome for SMEs.[171] The recurrent costs of self-assessment could be lower once internal capabilities have been put in place, while there would be higher recurrent costs for third-party assessment. In the context of the targeted survey, operating expenses (OPEX) – recurrent costs were estimated between EUR 3 000 and EUR 5 000 per product. Similarly, secondary data shows that the costs for internal testing for a laptop were estimated at EUR 5 000 per unit.[172] The stakeholders' feedback and estimated costs could be summarised as follows:

	Type of cost		
Testing method	*One-off costs*	*Recurrent*	*Average (estimation)*
Self-assessment	+/++	Neutral/+ (around 30%)	EUR 18 400
Third-party assessment	Neutral/+	++	EUR 25 000

The costs related to self-assesment and third-party assessment heavily depend on the complexity of the product, in particular in terms of supply chain involving different hardware and/or software manufacturers.

In order to estimate average costs, the following cost estimates from secondary data were used:

- In the Cybersecurity Act's Impact Assessment study,[173] it was estimated that costs (average recurrent and one-off) might potentially be higher than EUR 18 400 in staff costs, which corresponds to two FTE months for an average firm with an hourly rate of ca. EUR 29. No other secondary sources could be identified.
- For the *EU Cybersecurity Act*, in France the Certification Sécuritaire de Premier Niveau (CSPN) costs were estimated between EUR 25 000 to EUR 35 000, while in the Netherlands the Baseline Security Product Assessment (BSPA) were estimated on average at EUR 40 000.[174] For the delegated act of the RED, the cost estimations ranged from EUR 5 000 to EUR 50 000 or more, depending on the product.[175] Hence, an average of EUR 25 000 was chosen to estimate the costs of third-party assessment. As a matter of comparison, the benchmark averages in the Study to support the IA of the *Artificial Intelligence Act* lie between EUR 16 800 and 23 000[176].

Examples of testing costs for products[177]

- For testing connected garden equipment (consumer product), the costs would be of 25 000 EUR, while the BaU costs would be of only 20%.
- The costs of third-party assessment will increase with the complexity of the product, while for such products, the share of BaU costs would also typically be higher (70 to 90%). For example, for a more complex product, like a router, the total costs are estimated at EUR 126 000, with a BaU costs of 90%.
- For software intended for telecom networks and complex IT-systems (in the scope of policy option 4), self-assessment would cost around 30 000-50 000 EUR, with BaU costs of 90%.

Box 2: Costs of conformity assessment for policy option 3 and 4.

Policy option 4

[169] Several others stressed that such self-assessment should occur during the internal product development process, which would also allow to keep the costs low.
[170] Targeted survey launched on 16 May 2022 conducted by the study supporting this impact assessment.
[171] Idem.
[172] European Commission (2014): "Commission Staff Working Document, Part 2: Results of the case studies, A vision for the internal market for products", page 54, https://eur-lex.europa.eu/resource.html?uri=cellar:6da8f15b-8438-11e3-9b7d-01aa75ed71a1.0001.05/DOC_1&format=PDF.
[173] Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report
[174] SWD(2017) 500 final, IA accompanying the Cybersecurity Act.
[175] SWD(2021) 302 final, IA accompanying the RED Delegated Act..
[176] Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, final report (D5).
[177] SWD(2021) 302 final, IA supporting the RED delegated act

Under this policy option, all hardware and software manufacturers (depending on the sub-options), as well as distributors and importers, would bear additional compliance costs. As for policy option 3, the main costs for importers and distributors would be familiarisation costs. The costs of policy option 4 will depend on the sub-options related to the scope (4a) and (4b) and conformity assessment (i) an (ii). The detailed market analysis (*Annex 3*) did not enable to estimate the share of **critical non-embedded software**, therefore the assumption was made that it would represent less than 10% of the software market[178]. As in policy option 3, the market analysis did not enable to distinguish between embedded and non-embedded software, therefore the cost estimates are provided for the software market in general.

When asked in the public consultation about the costs of *introducing mandatory horizontal cybersecurity requirements for software products,* stakeholders indicated **medium to high costs** on average (3.68 out of 5). Hardware manufacturers rated the costs slightly lower (3.47) than software manufacturers (4.42 out of 5). As mentioned, for *introducing mandatory horizontal cybersecurity requirements for hardware products,* stakeholders indicated on average **medium to high costs** (3.55 out of 5). Taking the questions together, software manufacturers indicated in average "**high to very high costs"** (4.21 out of 5) compared to hardware manufacturers, who rated the costs "**medium to high"** (3.47 out of 5).

When consulting stakeholders, most respondents said that the impact of implementing security requirements relating to features of the products with digital elements and related to vulnerability management would be "**Medium"**, followed by "**High**".[179] The impact on costs of implementing requirements relating to security updates, end of life and whole life cycle would be **"High"**, followed by "Medium".

Under policy option 4, based on the available quantitative cost estimates,[180] and depending on the sub-options, the following **aggregated compliance costs** could be estimated:

Regarding **adjustment costs**, the same approach is taken as in previous sections on estimating secure product development costs: secondary data was used, which is the Venson calibration model that estimates an average of 30.5% additional product development costs if no comprehensive cybersecurity measures are in place (further explained in *Annex 4*). This leads to 42 700 EUR of additional product development costs for an average product with digital elements unit (140 000 EUR). The assumption that 50% of manufacturers are already implementing adequate security requirements (further explained in *Annex 4*) is taken.

The aggregated adjustment costs vary depending on sub-options related to the scope of the initiative. Under **policy option 4 a)** only 10% of the software market (assumption for share of critical software) would be impacted and the whole hardware market. By estimating the number of products with digital elements concerned using the SD and ICT-EXT-ADJ indicators, aggregated additional costs related to secure product development are of **EUR 6.11 billion**. Under **policy option 4 b)**, the full software and hardware markets would be impacted. By estimating the number of products with digital elements concerned using the ICT-EXT-ADJ and SD indicators, it leads to aggregated additional costs of **EUR 13.13 billion**.

As for policy option 3, costs for manufacturers, distributors and importers related to **familiarisation** could not be estimated, but would occur under all sub-options. The costs related

[178] The product categories that are considered to be critical will be defined in such a way that they should not represent a significant share of the market. Taking the whole market of products with digital elements, critical products with digital elements that need to undergo third-party assessment should be limited and not represent more than 10% of the total market. In order to estimate the costs, each time 10% of the total costs for the software market were added.

[179] Stakeholder workshop of 10 May 2022 organised by the study supporting this impact assessment, see Annex II.

[180] Several sub-options exist depending on the conformity assessment required, and whether only critical or all software would be covered. It was not possible to estimate the share of the software market represented by critical software, due to a lack of granularity in available market statistics. No distinction was made between option 4 (i) and 4 (ii**)** in terms of average costs related to testing given the lack of granular data, and it was assumed that no costs wold be passed on to the end-user.

to **information and transparency** for manufacturers to the end-users could not be estimated. According to the targeted survey[181], the impact on costs of implementing requirements related to transparency, guidelines and user information would be **"medium"**, followed by **"low"**. Respondents specified that the costs related to transparency and information would not be significant if provided in digital format.

Regarding the **conformity assessment costs**, they will vary for policy option 4 a) and b) depending on the sub-options related to conformity assessment. The average costs of testing by product with digital elements was drawn from secondary data, as explained in *Box 2*. These costs would be both adjustment costs in the case of self-assessment (e.g. setting up and maintaining testing facilities) as well as administrative costs linked to certification fees paid to notified bodies. The average cost for self-assessment was estimated at EUR 18 400, and for third-party assessment at 25 000 EUR (see *Box 2* above). As explained in policy option 3, the BaU factor for hardware manufacturers was estimated at 40%. For software manufacturers, it is assumed that the BaU factor would be lower, given that less software products are today covered by NLF legislation. In the absence of any data, an average BaU of 25 % was chosen, to reflect the feedback received from stakeholders that at least for more complex software products, testing, including third-party assessment, would be in place, and that testing was to some extent alredy carried out during the product development process.

Taking into account the BaU factor of 40% and 25% respectively for hardware and software products, and estimating the number of products based on the ICT-ADJ-EXT and SD indicators, the aggregated additional costs related to conformity assessment are summarised in the table below. It was assumed that third-party assessment would apply to 10% of the concerned products considered critical under policy options 4 (a)(ii) and 4(b)(ii).

In addition, the administrative costs related to documentation and reporting (e.g. technical documentation, declaration of conformity, affixing of the CE market and reporting of exploited vulnerabilites and cybersecurity incidents to ENISA), have been estimated with the followng assumptions: 9% of additional product development costs (see policy option 3); an average unit cost of EUR 140 000, and a number of products based on the ICT-ADJ-EXT and SD indicators. The results are summarised in the table below.

	Testing costs (adjustment and administrative costs)	Other conformity costs (administrative costs)	***Total conformity costs***	**Adjustment costs for secure product development**	**Total compliance costs** (adjustment and administrative costs)
4(a)(i) self-assessment	3.3 bn EUR[182]	EUR 3.6 bn	*EUR 6.9 bn*	EUR 6.1 bn	**EUR 13 bn**
4(a)(ii) third-party assessment	3.4 bn EUR - EUR 3 bn (self-assessment) - EUR 0.4 bn (third-party assessment)	EUR 3.6 bn	*EUR 7 bn*	EUR 6.1 bn	**EUR 13.1 bn**
4(b)(i) self-assessment	EUR 7.9 bn[183]	EUR 7.8 bn	*EUR 15.7 bn*	EUR 13.13 bn	**EUR 28.8 bn**
4(b)(ii) third-party assessment	EUR 8.1 bn - EUR 7 bn (self-assessme	EUR 7.8 bn	*EUR 15.9 bn*	EUR 13.13 bn	**EUR 29 bn**

[181] Targeted survey on impacts launched on 16 May 2022 organised by the study supporting this impact assessment
[182] self-assessment costs for hardware and 10% of the software market taking into account BaU costs and an average cost of EUR 18 400 EUR by company
[183] Self-assessment costs for hardware and software market taking into account BaU costs and an average cost of EUR 18 400 by company.

	nt) - EUR 1.1 bn (third-party assessment)				

Table 6: Overview of aggregated compliance costs on businesses by sub-option under policy option 4

Overview of benefits for businesses for all policy options

In policy option 1, the uptake of voluntary measures would be driven by market considerations (cost-benefit analysis) such as enhanced reputation as well as participation in public procurement procedures. It is likely that the manufacturers of the most problematic cheap equipment and software would not join a voluntary initiative as this would not be in line with their business strategy. The positive impact in terms of reduced cybersecurity incidents (*see section 6.6*), uptake of product with digital elements by EU users (*section 6.3.4*) and global competitiveness and innovation (*section 6.4*) would be limited and depend on the market uptake of voluntary initiatives. In addition, the absence of horizontal legislation would drive significant compliance costs and complexity (*see section 6.3*).

In policy option 2, similar to option 1, the positive impact in terms of cybersecurity incidents (*see section 6.6*), uptake of products with digital elements by EU users (*section 6.3.4*) and global competitiveness and innovation (*section 6.4*) would be limited to certain categories of hardware products, and if at all, to certain non-embedded software products used in a specific sector. In addition, the absence of horizontal legislation will drive significant compliance costs and complexity (*see section 6.3*).

In policy option 3, hardware manufacturers would benefit from a reduced number of cybersecurity incidents (see also *section 6.6*), although the impact would be limited by the fact that non-embedded software is not covered by a horizontal initiative in the first stage. The uptake of CE marked tangible products by EU users and globally is expected to increase (*sections 6.3.4* and *6.4*). The initiative would have a positive impact to prevent internal market fragmentation for all tangible products (*sections 6.3*).

Under policy option 4, both software and hardware manufacturers would benefit from a reduced reputational fallout following a decrease in the number of cybersecurity incidents of ca. 33% affecting their products (see also *section 6.6*). Furthermore, businesses would also benefit from enhanced supply chain security as users of products with digital elements. The uptake of CE marked software and hardware products would likely increase in the EU and globally, strengthening the EU's technological leadership. Furthermore, both software and hardware manufacturers would benefit from the prevention of internal market fragmentation (*section 6.3*).

As stressed by stakeholders in public and targeted consultations, in **policy option 3 and 4**, compliance costs could be substantially **off-set** by **alignment** with **existing European and international standards**. These standards will be taken into account in the standardisation process for harmonised standards that would follow the adoption of the initiative under policy option 3 and 4. The work related to standardisation is further developed under *Section 6.5*. It should also be noted that the compliance costs can be off-set by **transferring costs to the end-user**, which will be further developped under section 6.3.4.

Cost savings for businesses due to reduced cyber incidents under policy options 3 and 4

As a European regulation introducing horizontal requirements would trigger more than half of manufacturers to introduce a secure development product lifecycle, it is estimated that policy option 4 and 3 could reduce the cybersecurity attack surface of products with digital elements

respectively by between 20 % to 33 % for policy option 4 b) and by between 10 % and 16 % for policy option 3, and hence reduce the costs related to cybersecurity incidents for businesses.

These numbers are rough estimates of when the regulatory intervention would be fully applicable and the standardisation process has concluded. Assumptions include that currently less than 50% of manufacturers[184] (see also *Section 2.2*) follow a systematic approach to security and that a secure SDLC can reduce the number of critical vulnerabilities by 66 %. The latter number draws on a study showing that, after introducing its SDLC in 2004, Microsoft was able to reduce the number of critical vulnerabilities in its product by a range of 66 %[185] (see also *Section 6.5*). Furthermore, estimates of the share of incidents resulting from exploits against weaknesses in the computational logic and design of software range from 62 % to 90 % for operators of essential services identified under the NIS Directive[186]. It is assumed that this share is valid for the whole economy. Based on the market analysis presented in *Section 5.1.*, the hardware market, to which option 3 would apply at first, is estimated to make up 48 % of all products with digital elements, while the software market is estimated to make up 52 %. Under option 4 a), the market share of critical software is estimated to represent 10% of the software market[187]. Both under policy option 3 ii) and 4a)ii) or 4b)ii), it is not possible to make any assumption related to the impact of third-party assessement on vulnerability reduction and cost savings related to cybersecurity incidents.

Taking into account all the above-mentioned assumptions:

Under policy option 3, it can be estimated that the cybersecurity attack surface would be approximately decreased by 16%, if we assume that broadly all incidents are the results of vulnerabilities. This number takes into account that 50% of the hardware manufacturers (representing 48% of the concerned market) will implement a secure product development cycle. On the contrary, if considering that only 62% of the incidents are due to vulnerability exploitation, according to the lower estimate of the ENISA study mentioned above[188], this would lead to a reduction of the cybersecurity attack surface by 10%.

Under policy option 4 a), in addition to hardware manufacturers, 50% of the manufacturers of critical software would implement a secure product development cycle (taking into account the BaU). Critical software is estimated to represent 10% of the software market. Hence compared to policy option 3, it is estimated that the cybersecurity attack surface would be reduced by **11% to 18 %**, respectively reflecting scenarios where only 62% of the incidents are due to vulnerabilities or all incidents. This estimation leads most likely to an underestimation as critical software plays a specific role in the cybersecurity of products.

Under policy option 4 b), in addition to hardware manufacturers, 50% of the manufacturers of all software manufacturers would would implement a secure product development cycle. Hence, it is estimated that the cybersecurity attack surface would be reduced by **20 to 33%**, respectively reflecting scenarios where only 62% of the incidents are due to vulnerabilities or all incidents. This is a reasonable expectation, considering that building in security in the build-up of the product and ensuring effective vulnerability handling are the most effective means of addressing cybersecurity threats and incidents in products. As attackers usually need to chain multiple

[184] Security (2020): "Survey reveals nearly 50% of organizations knowingly push vulnerable software".
[185] Fonseca and Vieira (2013): "A Survey on Secure Software Development Lifecycles", *Software Development Techniques for Constructive Information Systems Design*, p. 12.
[186] Calculation based on the preliminary results of a still ongoing survey commissioned by ENISA and executed by Gartner (2022): NIS Investments Study 2022.
[187] which represents 38.853 companies ; the assumption is also used for the *compliance costs under Policy option 4* in the same section
[188] Calculation based on the preliminary results of a still ongoing survey commissioned by ENISA and executed by Gartner (2022): NIS Investments Study 2022

vulnerability exploits together to achieve their final objective, a reduction of vulnerabilities by 33 % could potentially thwart an even larger number of attacks.[189]

The initiative is designed to work in concert with the NIS2 Directive, which will require around 110 000 medium-sized and large firms to take appropriate security measures, including measures to prevent incidents. As a result, both the horizontal requirements for products with digital elements and NIS2 combined will lead to fewer vulnerabilities in products with digital elements, more security patches provided by manufacturers and faster patching of security holes by critical infrastructures and other essential entities.

In light of the above, option 3 could lead to a reduction of cybersecurity incidents by between 10 % and 16 % and as a result reduce the costs associated with cybersecurity incidents by a similar percentage. While estimates regarding the costs associated with cybersecurity incidents are not available at European level, data for certain Member States exists. Based on an extrapolation of incident-related data available for Germany (see *Box 3*), it is estimated that under this option the initiative could lead to a reduction in costs stemming from security incidents affecting companies by between **EUR 90 billion to EUR 140 billion annually**.

Option 4a), which would cover hardware and critical software, could lead to a reduction of cybersecurity incidents by **11% to 18%** and and reduced incident-related costs by a similar percentage. Using the data available for Germany (see *Box 3*), it is estimated that option 4 b) could lead to an EU-wide reduction in costs stemming from incidents affecting companies by between **EUR 97 billion to EUR 158 billion annually.**[190]

Option 4b), which would not only cover hardware but also software, could lead to a reduction of cybersecurity incidents by between 20 % and 33 % and reduce incident-related costs by a similar percentage. For instance, the annual costs associated with data breaches and DDoS attacks, which represent only a small subset of all types of security incidents, could be reduced by EUR 2.0 billion to EUR 3.3 billion and EUR 13.0 billion to EUR 21.45 billion respectively.[191] Using the data available for Germany, it is estimated that option 4 b) could lead to an EU-wide reduction in costs stemming from incidents affecting companies by between roughly **EUR 180 billion to EUR 290 billion annually.**[192]

There are no aggregate estimates of the cost of security incidents in Europe. The figures under PO3 and PO4 were calculated using **the cost of security incidents** in Germany as estimated by the German trade association Bitkom. The aggregated cost of security incidents in Germany amounted to EUR 220 billion in 2020 according to Bitkom (2021): "Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr". In order to calculate the aggregated benefits in terms of cost savings, the percentage of reduced cybersecurity incidents due to the policy intervention (as foreseen in the related policy option) is applied to the aggregated costs of security incidents in Germany and then extrapolated to the EU.

The aggregate cost of security incidents in Germany amounted to EUR 220 billion in 2020 according to the Bitkom (2021) study *"Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr"*. The data is based on a survey conducted by Bitkom Research on behalf of the digital association Bitkom. It surveyed 1 067 companies with 10 or more employees. The interviews were conducted with executives who are responsible for the topic of business protection in their company. These included managing directors and executives from the areas of corporate security, IT security, risk management or finance. The survey is representative of the economy as a whole. The study found out that nine out of ten companies (88 percent) were affected by attacks in 2020/2021 (compared to three quarters (75 percent) in 2018/2019).

[189] For example, if a specific privilege escalation vulnerability becomes unavailable, other stages of an attack, such as lateral movement and or data theft may no longer be possible.

[190] There are no aggregate estimates of the cost of security incidents in Europe. The figure was calculated using the cost of cybersecurity incidents in Germany and by extrapolation using the share of German GDP in European Union GDP. The aggregate cost of security incidents in Germany amounted to EUR 220 billion in 2020 according to Bitkom (2021): "Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr".

[191] According to the impact assessment of the delegate Radio Equipment Directive, the annual costs of data breaches are at least EUR 10 billion and the annual costs of DDoS are estimated to be at least EUR 65 billion.

[192] There are no aggregate estimates of the cost of security incidents in Europe. The figure was calculated using the cost of cybersecurity incidents in Germany and by extrapolation using the share of German GDP in European Union GDP. The aggregate cost of security incidents in Germany amounted to EUR 220 billion in 2020 according to Bitkom (2021): "Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr".

The table below summarises the estimations of all companies surveyed in the context of the Bitkom study that were affected in the last 12 months (prior to 2021: in the last 2 years) by theft, industrial espionage or sabotage (2021: n=935; 2019: n=801; 2017: n=571; 2015: n=550). These figures indicate direct and indirect sources of costs. For the purpose of this report, the assumption is taken that the theft, industrial espionage or sabotage impacting the German industry are direct and indirect consequences of cybersecurity incidents. For these reasons, using this figure will likely lead to an overestimation of cost savings for businesses due to reduced cybersecurity incidents.

Causes of damage	Loss amounts in billions of euros (2021)
Failure, theft, or damage of Information and production systems or operations	61.9
Extortion with stolen data or encrypted data	24.3
Data protection measures (e.g., informing customers)	17.1
Patent infringements (even before filing)	30.5
Loss of sales due to loss of competitive advantage	29.0
Loss of sales due to counterfeit products (plagiarism)	22.7
Damage to image among customers or suppliers/negative media coverage	12.3
Costs of investigations and substitute measures	13.3
Costs of legal disputes	12.4
Higher employee fluctuation/staff poaching	N.A.
Other losses	2.2
Total	223.5

Sources: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr ; Overview of the results of the survey: https://www.bitkom.org/sites/main/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf

Box 3: German study on economic impacts of security incidents

The upper-bound benefit of EUR 290 billion alone is estimated to be roughly ten times higher than the compliance costs (see *section 8*) and does not even take into account other non-quantifiable benefits, in particular under policy option 4, such as the decrease in risk mitigation costs for users; the higher uptake of digital solutions as a result of an increased trust in modern technologies; the reduction in risk mitigation costs (such as cybersecurity insurance) as a result of the reduction in the overall attack surface of products with digital elements; smaller reputational damage to manufacturers resulting from fewer incidents involving vulnerabilities in their products; enhanced productivity of manufacturers from a security point of view; and prevention of the potential costs of market fragmentation that manufacturers would be facing if Member States decided to intervene in the market.

The table below presents an overview direct costs and benefits described in this section (and further detailed in the following sections):

	Total direct compliance costs	**Benefits (direct and indirect)**
PO 1		
	Depending on the uptake of voluntary measures: • Secure product development costs (+30.5%) • EU certification (EUR 25 000 - 40 000)	Depending on the uptake of the voluntary measures: • Reduced cybersecurity incidents for end-users (decrease of vulnerabilities of around 33% by product) • Avoidance of costs related to security risk mitigation (e.g. insurance) for end-users • Increased uptake of products with digital elements by EU users and globally due to a reduction in risk associated with CE marked products with digital elements • Direct cost reduction for manufacturers that already use certification due to harmonisation
PO 2		
Amending sectoral NLF legislation	Secure product development (in average 30.5%	• Similar to PO1 depending on sectoral scope
Amending RED delegated Act	17.5 bn (for software only)	Limited to wireless products: • Reduced cybersecurity incidents for end-users • Reduction of costs and cybersecurity incidents

		• Increased uptake of products with digital elements in the EU and globally
PO 3		
3(i)	EUR 11.2 bn	• Reduced cybersecurity incidents for end-users (decrease of vulnerabilities of 33% by product): by **roughly EUR 90 bn to EUR 140 bn** • *Limited to the hardware market:* o Avoidance of costs related to security risk mitigation (e.g. insurance) for end-users o Increased uptake of products with digital elements by EU users and globally due to a reduction in risk associated with CE marked products with digital elements
3(ii)	EUR 11.3 bn	
PO 4		
4(a)(i)	EUR 13 bn	• Reduction in costs stemming from incidents affecting companies by roughly **EUR 97 bn to EUR 158 bn** • Avoidance of costs related to security risk mitigation (e.g. insurance) for end-users • Increased uptake of products with digital elements by EU users and globally due to a reduction in risk associated with CE marked products with digital elements
4(a)(ii)	EUR 13.1 bn	
4(b)(i)	EUR 28.8 bn	• Reduction in costs stemming from incidents affecting companies by roughly **EUR 180 billion to EUR 290 bn annually** • Avoidance of costs related to security risk mitigation (e.g. insurance) for end-users • Increased uptake of products with digital elements by EU users and globally due to a reduction in risk associated with CE marked products with digital elements
4(b)(ii)	EUR 29 bn	

Table 7: Overview of aggregated direct costs versus benefits for businesses by policy option 4

6.3.2. Impact on SMEs

SMEs will be significantly impacted by the initiative, both in terms of costs and benefits. They will be directly impacted by the new requirements as economic operators, i.e. as manufacturers, distributors or importers. Regarding manufacturers of products with digital elements, more than 99% are SMEs (see section 5). The share of SME distributors and retailers of products with digital elements could not be estimated. Furthermore, SMEs will be impacted by the initiative as end-users of products with digital elements. SMEs have been significant spenders in technology, with companies with less than 1 000 employees spending more than USD 30 billion a year on software alone.[193]

Policy option 1 is not expected to add significant costs on SMEs, while at the same time, SMEs may engage in voluntary measures to increase their market reputation. In the public consultation, SMEs rated the costs related to voluntary measures (guidelines, certification and public procurement) at respectively 3.4, 3.1 and 2.7 out of 5 (with 5 meaning very costly). Taking into account all organizations representing SMEs, the rating was similar (respectively 2.79; 3.00 and 2.87). European certification would significantly reduce costs and administrative burden for SMEs that already certify or are willing to certify their products and services at various levels of assurance. At the same time, benefits in terms of security for SMEs as end-users would be limited.

Under policy option 2, additional compliance costs would be borne by SMEs covered by the specific product regulation. In the public consultation, SMEs rated the costs with an average of

[193] nearly half of which is spent on vertical- or industry-specific software, including cloud: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/reversal-of-fortune-how-european-software-can-play-to-its-strengths

2.6 out of 5 (with 5 meaning very costly), lower than the average of other stakeholders (3.36). Taking organizations representing SMEs as a whole it was rated at 3.6. Furthermore, SMEs could face the costs of having to comply with multiple product specific legislations (*section 6.4*).

Under policy option 3, additional compliance costs would be borne by SME manufacturers, especially in the hardware segments that are currently not covered by product legislation, but also manufacturers of embedded software. Policy option 4 would in addition add compliance costs on SMEs software manufacturers. In the public consultation, SMEs rated the costs related to policy option 3 and 4 below or similar to the average. *Introducing mandatory horizontal cybersecurity requirements for hardware products* was rated at 3.55 out of 5 by all stakeholders in average (with 5 indicating very costly), while organizations representing SMEs in general rated it higher at 3.54. At the same time SMEs as end-users would benefit from greater legal certainty and more secure products in the hardware sector. SME companies rated the costs related to *Introducing mandatory horizontal cybersecurity requirements for software products*, at 3 out of 5 (the average was 3.68), while organizations representing SMEs rated it slightly higher at 3.59.

SMEs generally supported a level playing field between all companies. To the question on *whether small and medium-sized companies should be subject to the same obligations as larger companies*, organizations representing SMEs responded in average 3.92 out of 5 with 5 indicating that they strongly agree. Furthermore, in the public consultation SMEs did not consider that they would be disadvantaged compared to larger companies in a scenario of horizontal mandatory requirements (policy option 3 and 4). To the question on whether "*Mandatory cybersecurity requirements will put smaller hardware manufacturers and software manufacturers developers at a disadvantage compared with larger competitors"*, SME representatives were neutral (2.41 out of 5 with 5 indicating strongly agree). SMEs representatives were also neutral regarding the statement that EU companies are *at a disadvantage on the non-EU markets compared to non-EU competitors that are not subject to such requirements* (2.5 out of 5).

Several SMEs throughout the consultation activities expressed concerns that increasing the cost of development would possibly cause a competitive disadvantage vis-à-vis large companies and third countries. Some also expressed the fear that the compliance costs could not be borne by some SMEs, which might disappear from the market. SME representatives consistently called **for a proportionate approach and for supporting measures**. To the statement on the need to *Introduce simplified procedures to demonstrate conformity for small companies and individual entrepreneurs,* organizations representing SMEs replied on average at 2.79 out of 5 (with 5 indicating strongly agreed), while SMEs rated it in average at 3.7 out of 5. SME representatives stressed that SMEs would likely bear higher compliance costs and that these costs should remain proportionate and be reachable for SMEs. At the same time, stakeholders consistently stressed that any differentiation in terms of requirements and testing based on the size of the company should be avoided. Lighter administrative procedures and obligations could follow a risk-based approach and be based on the criticality of the product.

In terms of costs, **SMEs as manufacturers would in principle be more affected than large companies for several reasons**. Larger companies can more easily distribute the one-off costs of familiarising themselves with new regulation. Furthermore, larger companies have typically a larger customer base and can therefore distribute the fixed costs over more customers (economies of scale). Most importantly, SMEs' financial capacity to absorb fixed costs is much more limited.[194] First, SMEs might lack awareness and knowledge about cybersecurity in

[194] Estimates for 2018 produced by DIW Econ, based on 2008-2016 figures from the Structural Business Statistics Database, Structural business statistics overview: SMEs produce an average annual value added of EUR 174 000, going as low as €69 000 for micro-enterprises (less than ten employees), compared to €71.6 million for large enterprises.

general,[195] it might therefore be more costly for them to gather the knowledge about new security requirements, and to implement those. Due to limited internal technical and legal expertise, SMEs tend to turn to external consultants, increasing overall costs. Also, due to the limited capacity of their laboratories – as regards both economic resources and competences – SMEs have to use external testing laboratories or notified bodies to ensure compliance with applicable NLF-aligned legislation. According to a national trade association representing SMEs, 61% of SMEs report obstacles in ensuring their cybersecurity, the biggest challenges being inadequate skills and the costs of cybersecurity. According to an ENISA survey, approximately 12.3 % of the SMEs believe that their information security performance is 'below' or 'far below industry standards', compared to only 2.1 % for the large enterprises.[196] While these figures point to higher additional compliance costs, this also indicates the need to bring the security level of products manufactured by SMEs to an adequate security level.

Regarding policy options 3 (ii), and 4 a) (ii) and (b) (ii), **mandatory third-party assessment could entail considerable costs for SME manufacturer**, as highlighted by several stakeholders in the public consultation. One trade association representing SMEs mentioned that a too extensive scope of products to be covered by third-party assessment could have serious effects on specialised SMEs up to ceasing their activities. At the same time, other stakeholders in the targeted survey[197] mentioned that SMEs might prefer third-party assessment to avoid higher one-off costs for self-assessment. As a result, flexibility in choosing the conformity assessment seems important to offset the costs on SMEs.

It is important to note that not **all SME manufacturers will be impacted in the same way**. Some SMEs reported in the open public consultation and in conducted interviews that some costs could be covered by business as usual costs (e.g. some standards are already in place). Those SMEs that have no security measures in place will be the most impacted. However, it has not been possible to estimate the risks of market fall out due to excessive compliance costs for the SMEs.

SMEs as **importers and distributors** would bear some familiarisation costs, however as stressed by several SMEs representatives, these economic operators will benefit from the fact that "cybersecurity must already be ensured by the manufacturer". Therefore the burden on SME importers and distributors is not expected to be significant, on the contrary.

SMEs as end-users might also face higher initial prices, similar to other end-users (see section 6.2.4). However, these are not expected to be outweighed by the benefits of enhanced security and transparency (see below).

The following elements will help to off-set higher compliance costs for SME manufacturers, in particular under policy options 3 and 4:

- ✓ **Proportionality** of **security requirements and testing methodologies** was mentioned as essential by several SME representatives to avoid undue burden. Such a proportionate approach is foreseen under policy options 3 and 4. The essential cybersecurity requirements in the legislative proposal would be objective-oriented and proportionate building on widely used standards (such as ISO 27000 series and the IEC 62443 series, see *Annex 14*), and the standardisation process that will follow would take into account the technical specificities of the products. This means that for a given risk level, security controls would be adapted. Furthermore, the envisaged horizontal rules would only foresee third-party assessment for high-risk products. This would not represent more than 10% of the markets for products with digital elements. The impact on SMEs would depend on their presence in the market of the

[195] See also SWD(2021) 302 final, IA accompanying the RED Delegated Act.
[196] https://www.enisa.europa.eu/publications/nis-investments-2021
[197] Targeted survey on impacts launched on 16 May 2022 organised by the study supporting this impact assessment

specific product categories. Given the risk profile of these products, the BaU costs is expected to be high.

- ✓ Regarding the **proportionality of the costs for conformity assessment**, notified bodies conducting the third party assessments would take the size of the company into account when setting their fees, as it is currently the practice in NLF legislation.[198]
- ✓ Alignment of harmonised standards stemming from the initiative with **European and international standards** was stressed by SME representative as an important factor to reduce compliance cost. As previously mentioned, the EU standardisation process will build on existing standards.
- ✓ SME representatives stressed the need for **support measures**, while maintaining a level playing field between businesses. Such support measures could include the exchange of best practices and information sharing. They would stem from:
  - ➢ ENISA has put in place different tools to provide advice to SMEs in securing their business.[199] Other initiatives are under development, such as to self-assess the security maturity levels of SMEs. EU financial support will contribute to facilitate the implementation of EU regulation on cybersecurity (see *Annex 10*). For instance, EU programmes for research and innovation (Horizon Europe) and for capacity building (Digital Europe) and their respective precursor programmes aim to support EU know-how in security certification (in relation to the Cybersecurity Act) as well as capacity building and training, including for SMEs. The Digital Innovation Hubs funded from Digital Europe and National Coordination Centres under the Cybersecurity Competence Centre and Network regulation are resources for SMEs, which seek technical advice for product development or testing and/or EU cybersecurity financial support. In the 2021-2027 MFF period, Horizon Europe and Digital Europe will invest in the order of EUR 2 billion in a wide variety of cybersecurity topics and actions (see *Annex 10*).

On the other hand, SMEs are expected to benefit from the initiative in several ways, both as manufacturers and end-users, likely even more than large companies. First, as end-users, due to their limited capacities described previously, SMEs are likely to be more impacted by cybersecurity attacks, as evidenced by the open public consultation (OPC).[200] Furthermore, according to an ENISA survey, 90 % of the SMEs stated that cybersecurity issues would have serious negative impacts on their business, with **57 %** saying they would most likely become bankrupt or go out of business.[201] Therefore, while embedding security in products with digital elements would present a high compliance costs for some SME manufacturers, it would present significant cost saving for SMEs as end-users. SME as end-users would significantly benefit from enhanced transparency of security properties of products. As stated by a national trade association representing SMEs: "*In our experience, SMEs also often find it difficult to tell secure solutions and vendors from insecure ones due to the lack of transparency of cybersecurity features and standards. The absence of trust creates uncertainty and can result in SMEs holding back their much-needed investments in digitalisation".* As manufacturers, distributors and importers of products with digital elements, SMEs can benefit from larger trust from end-users and therefore possibly gain new customers. Larger companies typically already benefit from an established customer base, and therefore the benefits in terms of reputation could be even higher for smaller companies. A seamless access to the internal market with harmonised security requirements for all products with digital elements accross sectors can be even more beneficial

[198] SWD(2021) 84 final, Impact assessment accompanying the Artifical Intelligence Act.
[199] For instance, ENISA set up an online tool for SMEs (besides tips from ENISA, it also provides links and information from national efforts): https://www.enisa.europa.eu/securesme.
[200] As stated in the problem definition, SMEs and organisations representing SMEs rated the material and reputational impacts of cyber incidents higher than other stakeholders.
[201] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity

for SMEs, as they are less equipped to handle different regulatory requirements and related compliance costs.

6.3.3. Impacts on public authorities and notified bodies

A horizontal regulatory initiative will impact national authorities such as national accreditation bodies and market surveillance authorities (MSAs), as well as private notified bodies (i.e. notified conformity assessment bodies). These entities have responsibilities related to the monitoring and enforcement of the measures proposed under the different policy options. As the responsibilities of MSAs and notified bodies grow, their capacity to assess products' technical characteristics from a cybersecurity perspective need to be ensured. In this context, the need for appropriate skills (e.g. to assess software products) has been stressed as a key challenge by stakeholders.

Furthermore, next to the usual authorities involved in market surveillance under the NLF, ENISA will take over tasks in particular related to the collection and dissemination of exploited vulnerabilities in view of enhancing intelligence on cybersecurity threats to the internal market.

Direct costs for public authorities and notified bodies

Market surveillance authorities (MSAs)

The main cost sources for MSAs include: (i) possible creation of new authorities (one-off); (ii) familiarisation and training on the new requirements for existing or new authorities (one-off and recurrent for new staff), and (iii) enforcement of the new requirements, including post-market surveillance as part of life cycle approach (one-off and recurrent). In the long-term, cost-savings could occur thanks to a horizontal approach on security requirements (see *section 6.4*). The number of MSAs is still to be confirmed (discretion of Member States) and the precise impact will depend on the choices of Member States for the new MSA to be appointed under options 3 and 4. Different models can be envisaged by Member States in order to ensure that competent authorities would have the required expertise[202].

Under policy option 1, adjustment costs of market surveillance authorities would occur where a new certification or labelling mechanism is introduced. In the case of EU certification, market surveillance authorities already exist, i.e. the national cybersecurity certification authorities, however enforcement costs would occur if new schemes are deployed. When asked on the impact of voluntary measures in the public consultation, market surveillance authorities overall rated this option as **"very low"** (1/5 with 5 indicating very costly).

Under policy option 2, MSAs appointed under existing product legislation will need to adjust to additional requirements that include cybersecurity. On a case-by-case basis, additional resources will be required for enforcing new cybersecurity requirements on hardware products (e.g. additional physical checks of the products' technical characteristics and of the technical documentation against the minimum baseline security requirements). When asked in the public consultation on the costs of amending product specific legislation, public authorities acting as market surveillance authorities rated them **"high"** (4 out of 5 with 5 indicating very costly).

Under policy options 3 and 4, additional adjustment and enforcement costs would occur. The market surveillance authorities will be appointed by Member States and can differ from one Member State to another. The precise compliance and enforcement costs are thus difficult to estimate. When asked in the public consultation about the costs of horizontal legislation, public authorities acting as market surveillance authorities rated them **"high"** (4 out of 5 with 5 = very costly).

[202] *Final Report, Supporting Study for the evaluation of certain aspects of the New Legislative Framework (Decision No 768/2008/EC and Regulation (EC) No 765/2008), March 2022) - page 64 and 65*

In the context of the Cybersecurity Act,[203] it was estimated that Member States appointing a competent certification authority are expected to bear costs that would approximately amount to EUR 1 600 000 per year. This estimate includes costs related to personnel, equipment, subcontracting, operations as well as setting up of evaluation facilities. However, it is expected that most Member States would appoint existing authorities under policy options 3 and 4.

In order to estimate the enforcement costs, secondary data was used from the impact assessment of the delegated act of the RED[204]. MSAs stated that their estimated costs for enforcing the new (cybersecurity) requirements would be in the order of EUR 5 000 – EUR 10 000 for each type of simple equipment, and up to EUR 20 000 for each type of more complex equipment. In order to aggregate the costs, an **average costs by product of EUR 12 500** is estimated, and the number of products is estimated based on the ICT-EXT-ADJ and SD market indicators. Under policy option 3, the enforcement costs are likely to be lower when third-party assessment is implemented as market surveillance is carried out to some extent by notified bodies, however this difference could not be captured in the cost estimates. Hence, in average, under policy option 3 i) and ii), **aggregated enforcement costs for MSAs** are estimated of **EUR 3.1 billion**.

Under policy option 4, the enforcement costs would increase due to the broadened scope of products compared to policy option 3. As for policy option 3, the difference related to mandatory third-party assessment could not be captured. Under policy options 4 a) i) and ii), assuming that critical software represents 10% of the software market, the aggregated enforcement costs can be estimated at **EUR 3.6 billion**. Under policy options 4 b) i) and ii), the aggregated costs could be estimated at **EUR 7.7 billion**.

ENISA, the EU Agency for Cybersecurity

Under both policy option 3 and 4 and their respective sub-options, ENISA is tasked to receive notifications from manufacturers of actively exploited vulnerabilities contained in the products with digital elements, as well as incidents having an impact on the security of these products. Cost sources for ENISA would stem from collecting the information, from the preparation of intelligence on emerging trends regarding cybersecurity risks in products with digital elements to the national competent authorities and the European Commission, e.g in the NIS2 Cooperation Group, as well as from providing advice to support the implementation process of this Regulation. Such activities will involve additional adjustment costs for ENISA.

Drawing on the impact assessment of the NIS2 Directive[205], under option 4 b), collecting and disseminating information on exploited vulnerabilites to competent authorities could be estimated to require 3 FTEs. Any structured reporting and advice on the implementation of the initiative could add 1.5 additional FTEs. Taking into account the scope of the respective policy options, this amount could approximately be reduced to 2.5 FTE under option 3, and 3.5 FTEs under option 4a). These administrative costs would however be offset by reduced activities linked to the implementation of the European cybersecurity certification framework (as described in the policy options 3 and 4 in *Section 5*), and therefore would amount to budget re-allocation.

	Costs
PO 1	neutral/+
PO 2	++
Amending sectoral NLF legislation	
Amending RED delegated Act	*Aggregated enforcement costs for MSAs: EUR 4.6 bn
PO 3	
3(i)	*Aggregated enforcement costs for MSAs: EUR 3.1 bn

[203] SWD(2017) 500 final, IA accompanying the Cybersecurity Act.
[204] *Final report for RED Delegated Act Impact Assessment*, page 140
[205] https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union

3(ii)	* Vulnerability reporting for ENISA: 2.5 FTEs
PO 4	
4(a)(i)	*Aggregated enforcement costs for MSAs: **EUR 3.6 bn** - EUR 12 500 additional costs by new product *Vulnerability reporting for ENISA: 3.5 FTEs
4(a)(ii)	
4(b)(i)	*Aggregated enforcement costs for MSAs: **EUR 7.7 bn** - EUR 12 500 additional costs by new product * Vulnerability reporting for ENISA: 4.5 FTEs
4(b)(ii)	

Table 8: Overview of aggregated costs for public authorities by policy option

National accreditation authorities and notifying authorities

The main impacts for accreditation and notifying authorities will be linked to additional adjustment (e.g. additional training and human resources) and enforcement costs to take into account the new requirements. The resources spent by accreditation bodies in relation to NLF implementation are however **offset and borne largely by conformity assessment bodies through the purchase of accreditation services.** It is difficult to estimate the costs on national accreditation authorities and notifying authorities given their differences between Member States and their specificities (e.g. some are publicly funded, others private).

Under policy option 1, additional adjustment and enforcement costs for accreditation authorities would occur if a new European certification or labelling scheme is introduced. Under policy option 2, accreditation and notifying authorities would already be in place, but would bear adjustment and enforcement costs for accrediting conformity assessment bodies for cybersecurity requirements. Under policy options 3(i) and 4(i), self-assessment would be the rule, while third-party assessment would be optional for economic operators. Accreditation authorities will need to accredit notified bodies competent under the new legislation. This would lead to additional adjustment and enforcement costs, which would be mainly offset by fees paid by notified bodies. These costs are expected to increase with the extension of scope to non-embedded software (option 4) and if third-party assessment is mandatory (option 4 (ii)).

Notified bodies

Bodies that have been notified by the accreditation or notifying authority of a Member State have a key role in verifying the security and the compliance of products placed on the market. Notified bodies will mainly bear adjustment costs (e.g. training and new staff) and charges linked to the implementation of the new accreditation framework. These costs are both one-off (examination fee) and recurrent (annual fee to accreditation body and costs to develop a quality management system). The costs will partly depend on the processes in place and the availability of resources of the notified body. Fees will also differ depending on the accreditation body. In the context of the Commission evaluation of the NLF, the examination fee for accrediting a body, a one-off cost, was estimated between EUR 4 000 and EUR 20 000 per accreditation.[206]

Under policy options 2, 3, and 4, notified bodies will bear one-off and recurrent costs for adapting to expected changes. On an aggregated level, these will be more important under policy option 3 compared to option 2, and under policy option 4 compared to option 3

Benefits for public authorities and notified bodies

Policy option 1 and policy option 2 will have limited impacts for MSAs, accreditation bodies, national notifying authorities in terms of preventing internal market fragmentation (*section 6.5*). Furthermore, under these policy options, public authorities in general would have limited benefits in terms of security of products with digital elements (*section 6.3.4* and *section 6.6*).

[206] Draft European Commission (2022) Staff Working Document "Evaluation of the New Legislative Framework", Part 2/2 [to be published].

Under policy option 3 and 4, MSAs, accreditation bodies and national notifying authorities will benefit from the internal market effect of a horizontal intervention: harmonised security requirements for a wide range of products with digital elements instead of dealing with multiple national and/or European product legislation (see *section 6.5*). In addition, for accreditation bodies and national notifying authorities, costs will be offset by fees paid by notified bodies. While notified bodies will bear compliance costs, they will also benefit from an internal market effect. Furthermore, they will be remunerated for their conformity assessment services. In the context of the review of the Machinery Directive, increased turnover due to third-party assessment was estimated at EUR 202 million.[207] Public authorities in general will benefit as end-users from enhanced transparency on security properties and on secure use of products with digital elements and reduced compliance costs to meet other EU and national cyber relevant legislation (e.g. NIS) (*section 6.3.4*). They will also benefit from reduced cyber incidents and cyber mitigation costs (*section 6.6.*).

In addition, the burden on public authorities and notified bodies can be **partly offset by EU financial programmes** that have supported in the past MSAs, accreditation and notified bodies to facilitate the implementation of EU regulation on cybersecurity, and will continue to do so in the future (see *Annex 10*). As for SMEs (*section 6.3.2.*), EU programmes for research and innovation (Horizon Europe) and for capacity building (Digital Europe) and their respective precursor programmes support know-how in security certification (in relation to the Cybersecurity Act) and in relation to capacity building and training for competent authorities under the NIS Directive. In the same vein, and in order to partially offset potential costs related to the implementation of horizontal cybersecurity legislation, EU financial support will, subject to the respective programme governance decisions, support capacity building for public authorities and notified bodies. For a detailed overview, see *Annex 10.*

6.3.4. Impact on users: organisations, citizens and consumers

As described in *section 6.6.*, the mandatory security requirements for products with digital elements would lead to an increase in the security of hardware and software products, lowering the **risk of cybersecurity incidents** for both organisations (businesses and public administrations) and consumers as well as the customers of services that would be affected by fewer security incidents, such as data leaks. This would be in **particular beneficial to SMEs**, as several respondents to the public consultation pointed out that the negative impacts of cybersecurity incidents are more prominent for SMEs. Moreover, requiring manufacturers to document the security properties of their products would help users to make better purchasing decisions, allowing them to compare products-based security properties and individual security needs. While many users lack the necessary skills to analyse such information, it is very likely that consumer protection organisations, computer magazines, security consultants and other market actors would use this information to help users make informed choices. Similarly, requiring manufacturers to provide instructions on how to use products securely would empower users and ensure a more secure deployment of products.

As regards the impact on **risk mitigation costs** that businesses are facing, the measures are expected to lead to a decrease in such costs: business users could more confidently rely on the security of products with digital elements, knowing that the products have undergone a conformity assessment. According to a recent study by Gartner of behalf of ENISA, the initiative would have a very positive impact on key operators required to take cybersecurity measures

[207] SWD(2021) 82 final, IA accompanying the Machinery Regulation: based on the difference in cost for conformity assessment of third-party assessments compared to internal checks for 10% of products that currently undergo internal checks (Annex IV).

under the NIS Directive: 55 % of operators of essential services consider that the intervention would lead to a reduction in risk mitigation costs (i.e. cybersecurity investment).[208]

As described in *section 2.1*, users forgoing investment in products with digital elements is one of the consequences of the low level of security provided by products with digital elements. With users and in particular businesses becoming more confident in the security of products with digital elements, the initiative would therefore also lead to an increased **uptake in digital solutions**.

As regards business users, the initiative would lower the **compliance costs with existing legal acts**, such as the NIS Directive or the GDPR, in particular when it comes to supply chain security requirements: In the aforementioned Gartner study, 71 % of operators of essential services consider that the intervention would lead to a reduction in supply chain security compliance costs.[209]

Finally, as the manufacturers of products with digital elements will be facing compliance costs to implement cybersecurity requirements, they are likely to pass on some of these costs to users, leading to an **increase in prices** for consumers as well as organisations. However, this is not expected to have a significant impact. When asked in the public consultation whether they *valued products' usability and price over cyber security features*, 46 % of respondents disagreed and only 12 % seemed to privilege usability and price over cyber security. The results were similar for SMEs.[210] Based on the impact assessment of the RED delegated act, for lawnmowers, the additional costs for end-users could be up to 3 EUR per unit more expensive compared with a non-secured lawnmower product with cheap Wi-Fi connectivity. Integrated encryption into the Central Processing Unit (CPU) would require changes to the electronics and additional technical support, which could result in extra costs to the end-user of up to 10 EUR per unit. The price increase per router for testing would be up to EUR 0.355 per device.

In addition, transparency requirements would contribute to boosting the awareness of users of the security risks associated with certain products. Consumer protections organisations and other actors, such as security researchers or computer magazines, could use the additional information provided by manufacturers to provide consumers and organisational users with a better overview of the security properties and features of products with digital elements, helping them make better purchasing and deployment decisions.

Under policy option 1, the positive impact on users in terms of security, risk mitigation, digital uptake and compliance costs would be limited, considering that no mandatory measures would be imposed. However, additional certification schemes could incentives certain players to undergo ICT product certification, boosting confidence of users in such products and lowering businesses' compliance costs with other legislation. Under policy option 2, there would be a positive impact on users for a limited number of products covered by the NLF legislation. However, the majority of products with digital elements in the EU are currently not covered by any NLF legislation. A more substantial impact would occur if the scope if the RED Delegated Act is extended to non-emebedded software. Under policy option 3, which includes a horizontal regulatory intervention for a broad scope of tangible products with digital elements, the positive impact on users in terms of security, risk mitigation, digital uptake and compliance costs would increase dramatically as regards tangible products. It would however remain very limited as regards software products. Under policy option 4, all manufacturers of tangible and intangible products would be expected to take cybersecurity measures, which would lead to a substantial

[208] Calculation based on the preliminary results of a still ongoing survey commissioned by ENISA and executed by Gartner (2022): NIS Investments Study 2022.
[209] See previous footnote.
[210] Medium companies were mostly neutral (43%) and disagreed (47%); small companies disagreed (42%), were neutral (33%), but also partially agreed (17%); micro companies tended to disagree (30%) or be neutral (40%).

positive impact on users, citizens and consumers in terms of security, risk mitigation, digital uptake and compliance costs with other legislation. In the public consultation, when asked whether *Horizontal cybersecurity requirements for products with digital elements would increase awareness of users when it comes to cyber risks,* 82.22 % of respondents (strongly) agreed.

6.3. Functioning of the internal market

The impact on the internal market depends on how effective the regulatory framework is in preventing the emergence of obstacles and fragmentation by mutually contradicting national initiatives aiming to address the problems set out in *section 2.1*.

Member States are increasingly recognising the need to address concerns regarding the security of products with digital elements. For example, in 2019, Finland has created a labelling scheme for IoT devices, such as smart TVs, smartphones and toys based on the ETSI standards.[211] Germany has recently introduced a consumer security label for broadband routers, smart TVs, cameras, speakers, toys, as well as cleaning and gardening robots.[212] Policy options 1 and 2 explicitly point to the creation of additional voluntary national schemes absent Union legislation.

So far, mandatory national cybersecurity requirements for products with digital elements are rather the exception than the rule in the Member States. One notable example is the mandatory protection profiles introduced by Germany for manufacturers of smart meter gateways.[213] Given the dire state of product security in the internal market, Member States are expected to sooner or later consider further national product rules to protect their critical infrastructure, crucial manufacturing processes or citizens. Such a national approach would inevitably lead to a fragmentation of the internal market.

Most products with digital elements markets are European if not global. Major operating systems, such as Microsoft Windows or Android with its various forks, are sold to a global user base. Similarly, given the importance of economies of scale in hardware markets as described in *section 2.2.5*, many components, such as CPUs or network chipsets, are equally marketed across the globe. For example, infected IoT devices in the internal market can be traced back to the same manufacturers, irrespective of in which Member State they are deployed.[214] National rules on such products would therefore force manufacturers to adjust their products to national markets, resulting in a decrease in cost-effectiveness across the internal market. In some cases, manufacturers, and in particular smaller ones, may even decide not to market a product in regions with a low expected sales volume in order to avoid the additional cost associated with adjusting the product to national rules.

While policy options 1 and 2 may entail additional voluntary national schemes as one way of addressing the problem of low product security, nothing would prevent the Member States from setting their own rules with the negative consequences described above. In the public consultation, when discussing the impacts, multiple stakeholders expressed the dangers of legislative fragmentation, and mentioned that any interventions that foster fragmentation (voluntary vertical schemes or national regulatory schemes) will drive significant compliance costs and complexity to no improved security. Under policy option 2, internal market fragmentation could at least be prevented for those products that are regulated under the NLF. However, in the public consultation, several stakeholders mentioned that amending different legislation with cybersecurity requirements would lead to a multiplicity of non-homogeneous

[211] ETSI EN 303 645 standard. Traficom (2019).
[212] BSI (2022).
[213] German Metering Point Operation Law ("Messstellenbetriebsgesetz", MsbG), §22.
[214] Rodríguez et al (2021): "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", *20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, for a more detailed discussion of IoT consumer device security,
p. 8.

requirements and increase the overall cost. Policy option 3 would effectively prevent internal market fragmentation for all tangible products, given its horizontal regulatory intervention in this area. Given its staggered approach to the introduction of security requirements for non-tangible products, internal market fragmentation in the area of software would most likely be temporary. Policy option 4 would be the most effective in preventing fragmentation, as the horizontal regulatory intervention would cover a broad scope, including all software. In the public consultation, to the question whether "*Horizontal cybersecurity requirement would improve the functioning of the internal market by levelling the playing field for manufacturers […]",* over 88 % respondents strongly agreed.

6.4. Competitiveness, innovation and trade: Impacts on EU and non-EU companies

Competitiveness and trade in the software and hardware markets

Competition in the software market is generally global and the sector is a highly profitable one. Software is used to a large extent from external providers, either as a ready-to-use system or via hired external contractors. Therefore, companies from outside the EU find it relatively easy to win customers, and as a result supply chains are often international. The EU is importing more than exporting software products. In percentage terms, the software share of extra-EU exports is separated from that of intra-EU27 imports by **18 %** (see *Annex 3*).

Regarding hardware, EU imports from third countries and intra-EU imports are similar shares, with intra-EU imports only surpassing extra-EU ones by five percentage points. The competitiveness of EU products and commercial balance might vary from one sub-category of hardware product to another. In 2021, several product categories that are amongst the top EU export products could be covered by a possible horizontal regulatory intervention such as: machinery and equipment (12.9 % of total exports), and computer, electronic and optical products (7.9 %).[215] Amongst the top EU imports are: computer, electronic and optical products (14 % of total imports); machinery & equipment, electrical equipment and basic metals (all three 6 %).

Possible impacts on EU and non-EU companies in terms of competitiveness

Regarding the impact on **EU companies**, on the one hand, additional compliance costs could increase the development and production costs of EU companies and hence their ability to export products globally. Furthermore, conformity assessment might delay the placing on the market of a product with digital elements, and hence the first mover advantage. On the other hand, the initiative can impact positively the uptake of products with digital elements globally and enhance the productivity and reputation of European companies from a security standpoint, thereby contributing to Europe's position as global leader in cyber-secure products.

Under policy options 1 and 2, the impact on Europe's competitiveness would be limited, both in terms of possible compliance costs and benefits. Given the voluntary nature of the measures, the impact of these options on reputation is expected to be limited to those manufacturer that decide to engage into voluntary measures, such as national labelling and EU certification. The absence of any "CE mark" or alike for a substantial part of the hardware and software market will however reduce the impact on enhancing the reputation and visibility of EU products with digital elements globally (and similarly, non-EU products with digital elements offered on the EU market). The increased demand for products with digital elements would depend on the extent to which voluntary measures penetrate the market.

Under policy option 3, and policy option 4, additional compliance costs would occur respectively for European and non-EU hardware and embedded software manufacturers as well as non-embedded software manufacturers. However, it is expected that these policy options would

[215] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Main_goods_in_extra-EU_exports

equally strengthen the visibility and reputation of EU hardware and if applicable software products globally as well as of non-EU hardware products on the EU market in terms of cybersecurity

When asked in the public consultation on whether *Mandatory cybersecurity requirements will put EU manufacturers at a disadvantage on the non-EU markets compared to non-EU competitors that are not subject to such requirements,* hardware manufacturers were neutral (2.6 out of 5, with 5 indicating strong agreement), while software manufacturers generally agreed (3 out of 5). Organisations representing SMEs had a neutral stance (2.5 out of 5), and SME companies generally disagreed (2 out of 5). This suggests that software manufacturers could be slightly more concerned regarding the impact on their global competitiveness. In this context, mention should be made that the responses of software developers must be analysed in a wider context, considering that, unlike hardware manufacturers, they have been very limitedly exposed to NLF-type legislation, if at all. Stakeholders stressed the concern that horizontal requirements could undermine the winner-takes-all dynamic, which is by nature even more prevalent in the software sector (or first mover advantage). In particular, third-party assessment under option 4(ii) can delay the timing of placing an EU software product on the global market. However, these impacts are not expected to be significant as only very limited categories of products would be affected by such third-party testing. When asked in the online targeted survey on whether policy option 4 would *negatively affect exports of products with digital elements at industry level*, respondents mentioned a low impact (2.4 out of 10 with 1 being the lowest and 10 the highest). Respondents rated the *negative impact on imports* slightly higher, but still not significant (3.7 out of 10). Furthermore, both under option 3(ii) and 4(a)(ii) and 4(b)(ii), third party assessment could only apply to a very narrow share of products (max. 10%), for which the BaU cost are likely to be high.

A horizontal initiative under policy option 3 and 4 can be beneficial to the European industry, as it would raise the overall security culture in Europe, making European products with digital elements more secure, reliable and trustworthy, and hence competitive. The demand for products with digital elements will continue and/or might even increase on the EU market, and security is an increasing driver of this demand. Hence, a horizontal initiative could contribute positively to build Europe's global technology leadership in the hardware and software market. Assurance on security requirement are both attractive in the B2B sector and B2C sectors.[216]Furthermore, as highlighted in the Commission's sector inquiry on Internet of Things[217] cybersecurity is a key parameter on which consumer IoT manufacturers compete.[218] Experts also highlight that growth for European companies in the software could result by exploiting the competitiveness of the European software industry in the vertical industrial sectors and B2B segment.[219] In this context, assurance on security could provide a competitive strength to European B2B software products in a large number of sectors. Similar to other NLF legislations, a horizontal regulatory intervention is expected to enhance the quality and reputation of "CE marked" hardware and

[216] https://ec.europa.eu/competition-policy/system/files/2022-01/internet-of-things_final_report_2022_staff_working_document_0.pdf
[217] https://ec.europa.eu/competition-policy/system/files/2022-01/internet-of-things_final_report_2022_staff_working_document_0.pdf
[218] See paragraph 114: Manufacturers of smart home devices indicate that the quality, cybersecurity, brand reputation and privacy policy of their own devices play a crucial role when competing with other smart home devices for integration with other devices, services, voice assistants and other smart home user interfaces.
[219] The annual global market for vertical software, which powers industry-specific processes, currently stands at around USD 100 billion and is expected to grow at an annual rate of some 19 % over the next five years: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/reversal-of-fortune-how-european-software-can-play-to-its-strengths

software offered on global markets, and therefore bring competitive strength to European manufacturers compared to their third country counterparts.[220]

A horizontal initiative will have positive effects on innovation in cybersecurity technologies in Europe and boost the competitiveness of European industry. The introduction of security requirements, such as security by design, as well as conformity assessment, as well as the definition of related harmonised standards (or if applicable, specifications by the Commission) will provide legal certainty for investments and boost the demand for a variety of cybersecurity tools, such pen testing, automatic scanning, etc. Those technologies have been identified as priorities for investments in R&D under Horizon Europe (see *Annex 10)*. At the same time, as regards the effects on innovation in general, the intervention would be proportionate and would introduce objective-based requirements, technology and product/sector-neutral, without being overly-prescriptive. A reasonable transition period of 2-2.5 years to prepare the implementation would also be provided (see standardisation below), giving time to the relevant markets to prepare, while providing a clear direction for R&D investments.

The **impact on non-European companies** will be similar to the one on European companies. Given its large share of imports, the EU is an attractive market for non-EU companies. Therefore, exporting to Europe will likely remain attractive for non-EU companies. While it cannot be excluded that some firms might direct their offering to other markets, this effect is not expected to be significant. Furthermore, the initiative could enhance the reputation of non-EU providers on the EU market by demonstrating that they are meeting high security standards. A significant cost could stem from the obligation to have an economic operator established in the Union, which exists in some NLF legislation. However, this is not envisaged in any of the policy options. Last, it is important to stress that while European horizontal requirements for products with digital elements would be the first comprehensive product security initiative globally, EU trading partners, with the US in the lead, are pursuing similar objectives to the EU with regard to security of products with digital elements and have started to introduce measures to address particularly the security of supply chain and security of products with digital elements. (see *Annex 6*).

The role of standardisation in competitiveness and innovation

Under the policy options (3) and (4), following the adoption of the legislation, the Commission will prepare a **standardisation request** (under Regulation 1025/2012 on European standardisation) to the relevant **European standardisation bodies** (ESOs), ETSI and CEN-CENELEC[221], taking account of a transition period from entry into force to application of at least two years to allow the preparation of implementation, including the development of needed harmonised standards by ESOs.

Stakeholders consistently stressed that both EU and non-EU companies that are operating globally would greatly benefit in terms of competitiveness if EU standards and conformity assessment methodologies are as much as possible **aligned with existing European and international standards**. For global (EU and non-EU companies), possible costs could stem from regulatory divergence between the EU and global trade partners. The costs of third party conformity assessment and certification could risk being duplicated across different regulatory jurisdictions if EU rules diverge from each other and from international ones.

[220] "According to evaluations of certain NLF legislation, such as the Lifts Directive evaluation, the CE marking is increasingly perceived as a standard of quality by industry beyond EU borders: buyers in Asia and the US are reported to prefer products with a CE marking; also, the harmonised regulatory framework has reportedly helped companies implement a stronger internationalisation strategy in third countries. The EMCD evaluation reached similar conclusions." Final Report, *Supporting Study for the evaluation of certain aspects of the New Legislative Framework (Decision No 768/2008/EC and Regulation (EC) No 765/2008)*, March 2022

[221] These European standardisation bodies have also been recognised as competent in the context of the RED delegated act.

The ESOs pointed out that the cost of developing standards is financed primarily by industry (93-95%) followed by national governments (around 3-5%) and the European Commission / EFTA contribution (around 2%)[222]. The approximate cost of creating one standard from scratch was estimated at approximately **EUR 1 million**. The cost is financed primarily by industry (93-95%) followed by national governments (around 3-5%) and the European Commission / EFTA contribution (around 2%)[223]. Compliance with harmonised standards is not mandatory, but creates a presumption of compliance with the legal requirements, unless otherwise specifically provided by the horizontal regulation. This creates a strong incentive for industry to contribute to the standardisation work, which is always a voluntary process. The fact that industry bears most of the cost of the system, together with the voluntary character of standards, reflects its high interest in the role of standards, including in support to the application of NLF-aligned legislation. If developed in a timely manner, harmonised European standards can provide a key competitive advantage for European industry by adopting more advanced standards compared to their competitors.

However, it has to be noted that, recently, economic operators and business associations mentioned the development of harmonised standards as a severe issue, generating significant costs for companies beyond the costs associated with the development of standards detailed above. Companies face difficulties in using new standards, reportedly due to delays in the mandates by the Commission and the citation of harmonised standards at EU level: this ultimately hampers companies' competitiveness, as competitors on the global stage (for instance, in the United States and China) adopt more advanced standards than Europe[224].

The alignment with existing and international standards would be ensured in the following ways:

- ✓ The Commission will request the harmonised standards to be developed on the basis of the European horizontal regulation will take account (e.g. through a gap analysis) existing international standards and all other relevant standards developed by that time, including those on the basis of the RED delegated act[225]. The envisaged requirements for the proposal for a horizontal regulation should take into account of the main elements of the standardisation request to be issued on the basis of the RED delegated act.
- ✓ In order to ensure alignment with existing cybersecurity standards, ENISA should be involved in the standardisation work.
- ✓ The adoption of harmonised European standards does not mean that new standards need to be built from scratch. An existing standard can be designated as harmonised standard for presumption of compliance with essential requirements defined in the Union legislation. While there are existing standards related to the security of products with digital elements (see table in *Annex 13*), only a detailed gap analysis would enable to conclude if some standards would provide the required level of security.
- ✓ The EU has already announced the willingness to work closely with its main trading partners, in particular the US to deepen its cooperation "on new cybersecurity technologies and standards".[226]

[222]Final Report, *Supporting Study for the evaluation of certain aspects of the New Legislative Framework (Decision No 768/2008/EC and Regulation (EC) No 765/2008)*, March 2022
[223]Final Report, *Supporting Study for the evaluation of certain aspects of the New Legislative Framework (Decision No 768/2008/EC and Regulation (EC) No 765/2008)*, March 2022
[224] Final Report, *Supporting Study for the evaluation of certain aspects of the New Legislative Framework (Decision No 768/2008/EC and Regulation (EC) No 765/2008)*, March 2022
[225] See EC standardisation request for RED delegated act: https://ec.europa.eu/docsroom/documents/48359
[226] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_2007

6.5. Security and resilience

While there is little systematic research measuring the effect of a Security Development Lifecycle (SDLC) on product security, available evidence suggests that firms can significantly reduce the attack surface of their products by implementing a systematic approach to cybersecurity in their development processes. For instance, after introducing its SDLC in 2004, Microsoft was able to reduce the number of critical vulnerabilities in its product range by 66 %.[227]

As regards securing products across the entire life cycle, in particular by providing timely security updates for critical vulnerabilities, Google's Project Zero provides evidence that manufactures can indeed provide security updates much more quickly than under the status quo, if provided with proper incentives. Amongst the software projects that Project Zero is analysing, the number of days between the discovery of a vulnerability and the provision of a fix has dropped from an average of 80 days to 52 days.[228] A legally binding requirement covering the entire hardware and software market would produce strong incentives to reduce the time for providing security updates.

Information regarding the actual implementation of SDLC by hardware and software manufacturers is patchy. According to a 2010 survey conducted amongst 46 manufacturers, only 30.4 % of them have implemented a formalised approach.[229] More recent studies focusing on Europe, produce similar findings: A survey of Norwegian public organisations involved in developing software concludes that on average only 39 % of the security measures described in the Building Security In Maturity Model (BSIMM) are implemented.[230] In a 2021 study amongst 61 Finnish software practitioners, 29 % of respondents said their firms were not following any systematic approach.[231] Based on this data, it is estimated that currently less than 50 % of manufacturers have a systematic approach to product development.

Given the low uptake of secure coding practices by manufactures, the introduction of mandatory requirements as regards the security of products and development processes would lead to a significant increase in product security and, as a result, in the security and resilience of users, including critical infrastructures, other providers of essential services and consumers. A survey conducted as part of the NIS Investments Study 2022 shows that developing more secure products and patching holes in existing products would substantially lower the costs associated with cybersecurity incidents: 69 % of critical infrastructure providers and other operators of essential services stated that mandatory cybersecurity requirements for products with digital elements would lead to a reduction in the number of security incidents, suggesting that the intervention would significantly contribute to raising the level of resilience of the most critical parts of the European economy.[232]

Experience has shown that mandatory security requirements are indeed effective in making companies take security more seriously and ultimately in raising the overall level of security. In a 2020 survey assessing the impact of the NIS Directive on security, 82 % of operators of essential services gave the Directive a mark of 4 or above (on a scale from 1 to 5).[233]

---

[227] Fonseca and Vieira (2013): "A Survey on Secure Software Development Lifecycles", *Software Development Techniques for Constructive Information Systems Design*, p. 12.
[228] https://googleprojectzero.blogspot.com/2022/02/a-walk-through-project-zero-metrics.html.
[229] E.g. Microsoft's Security Development Lifecycle or the Comprehensive, Lightweight Application Security Process (CLASP): Geer, D. (2010), p. 12-16.
[230] Martin Gilje Jaatun et al (2015): "Software Security Maturity in Public Organisations", *ISC 2015: Proceedings of the 18th International Conference on Information Security - Volume 9290, September 2015*, p. 120-138.
[231] Kalle Rindell et al (2021): "Security in agile software development: A practitioner survey", *Information and Software Technology Volume 131, March 2021, 106488*.
[232] Calculation based on the preliminary results of a still ongoing survey commissioned by ENISA and executed by Gartner (2022): NIS Investments Study 2022.
[233] ENISA (2020): "NIS Investments Report 2020", p. 34, https://www.enisa.europa.eu/publications/nis-investments/.

Under policy option 1, the number of hardware and software manufacturers that would introduce a SDLC and provide security updates throughout a product's life cycle is unlikely to increase, considering that the additional guidance provided by the Commission would be just one more non-binding recommendation.[234] Under policy option 2, the number could only increase for manufacturers of products covered by NLF legislation and possibly very limited categories of non-embedded software products. Policy option 2 would therefore not provide any additional security for a wide range of critical products, and in particular for non-embedded software, which would remain largely unregulated from a security standpoint. Under policy option 3, the number would increase dramatically for manufacturers of tangible products, as manufacturers would only be able to meet the requirements laid down by the EU horizontal rules by implementing a formalised approach to product security. As regards software manufacturers, they might eventually be required to take a systematic approach to security too (staggered approach). Under policy option 4 b), all manufacturers of tangible and intangible products across the entire supply chain would be expected to take a systematic approach, which should lead to a substantial increase in product security, as manufacturers would not only need to take the security of processes and products seriously before the placing on the market, but they would also have to introduce adequate vulnerability management measures, provide security updates beyond the placing on the market and make information available to users helping them to choose the products with the best security properties and use these products in a secure way. These measures would be entirely absent from policy option 1 and only apply to a limited range of products under policy options 2 and 3. In the public consultation, regarding the question whether *Horizontal cybersecurity requirements for products with digital elements would enhance and ensure a consistently high level of the security of products with digital elements,* over 90 % of the respondents (strongly) agreed.

6.6. Impacts on fundamental rights

All policy options are expected to enhance to a certain extent the protection of **fundamental rights** and freedoms such as privacy, protection of personal data, conduct of business and property or personal dignity and integrity. Policy options 3 and 4 consisting of horizontal regulatory interventions are nevertheless expected to be more likely to help decrease the number and severity of incidents, including personal data breaches. In particular, policy option 4 covering the broadest scope, including all software would be the most effective in this regard.

The horizontal cybersecurity requirements would contribute to the security of personal data by protecting the confidentiality, integrity and availability of information in products with digital elements. Compliance with those requirements will facilitate compliance with the requirement of security of processing of personal data under the GDPR. Certain requirements, such as security by design and default, will also contribute to making the products more data-protection and privacy-friendly from the design phase. A horizontal intervention, and notably the most comprehensive in scope, i.e. option 4 b), would enhance the transparency and information to users, including those that might be less equipped with cybersecurity skills. Users would also be better informed about the risks, capabilities and limitations of the products with digital elements, which would place them in a better position to take the necessary preventive and mitigating measures to reduce the residual risks.

At the same time, the significance of the impacts on the protection of fundamental rights will depend on the degree of regulatory intervention, as presented below.

[234] In addition to existing international standards, such as IEC 6244, which addresses cybersecurity for operational technology in automation and control systems, or ETSI TS 103 732, a protection profile for consumer mobile devices, a number of guidance documents has been developed by industry, such as Microsoft's Security Development Lifecycle. For a comprehensive list of guidance documents, see Yasemin Acar et al (2017): "Developers Need Support, Too: A Survey of Security Advice for Software Developers", *2017 IEEE Cybersecurity Development*, p. 24.

Respondents to the open public consultation have rated the actual impact of a damage to fundamental rights caused by a cybersecurity incidents affecting products with digital elements as moderate to high, with an overall average rating of 3.8 (on a scale of 1 to 5), a 4.16 rating by users and 4.5 by consumer organisations. SME companies gave an overall rating of 4.

As regards the overall impact of cybersecurity requirements on fundamental rights, the respondents to the public consultation consider that they would enhance the protection of privacy and personal data to a high degree (an average of 4.09 on a scale of 1 to 5). SMEs rated the impact similarly at 4.1. The respondents also agreed to a great extent that the requirements would ensure a high level of consumer protection[235]. SMEs also rated the impact high (4.4 out of 5).

6.7. Social impact

Cybersecurity incidents have far-reaching consequences for society. Therefore, enhancing the cybersecurity of products with digital elements would also have positive social impacts such as reduced levels of cybercrime. Moreover, improving the transparency and information of users would have positive impacts for more vulnerable groups of users. Also, the initiative would have a positive effect on the labour market by creating new opportunities for cybersecurity trained specialists.

It is expected that policy options 3 and 4 would ensure a higher level of cybersecurity for products with digital elements and would therefore have a stronger impact in the prevention of cybercrime and on social aspects in general. Since policy option 4 a) and b) would cover also standalone software (only critical for 4 a)), considering the particular relevance of such products (such as apps) with strong social aspects, it would be expected that the positive impact of this policy option in this regard would be the highest.

In addition to the four problem drivers addressed by the Commission's planned intervention, three additional drivers were identified: "lack of bargaining power of users", "lack of qualified security professionals" and "lack of cybersecurity awareness and skills of users". While the initiative would not address those additional drivers directly, policy options 3 and 4 would contribute to a European security culture. Moreover, the additional efforts by manufacturers in raising the level of security of their products could further increase the demand for security professionals and would incentivise more citizens to consider a career in cybersecurity. Finally, as citizens would see the CE marking affixed to a wide range of products having undergone conformity assessment, the intervention would also lead to an increased awareness of the risks associated with products with digital elements, creating incentives for citizens to improve their understanding of cybersecurity issues.

The consultation activities revealed that policy options 3 and 4 are expected to create to the greatest extent additional jobs in the relevant markets and in the whole economy (respectively scoring an average of 5.0 and 6.4 on a scale from 1 to 10 for the former and 5.6 and 6.6 for the latter). Policy options 3 and 4 are also considered to increase the demand for additional or new skills to the largest extent (respectively scoring an average of 6.6. and 7.4 on a scale from 1 to 10).

6.8. Environmental impacts

Strengthening the cybersecurity of products with digital elements could have positive environmental impacts by contributing to wider use of latest generation digital infrastructure and services, which are more sustainable and compliant with the latest environmental standards.

Incidents affecting critical infrastructure and manufacturing could in some instances have a negative impact on the environment, as incidents could result in harmful emissions, waste

[235] an average of 4.04 on a scale of 1 to 5.

discharges as well as spills.[236] Even though not many such incidents have occurred so far, cybersecurity experts consider the risk to pipelines or other critical infrastructure to be real.[237] Depending on the policy option, the regulatory intervention could therefore prevent environmental damage by having a positive impact on the resilience of such entities, as it would improve the security of SCADA systems and other hardware and software deployed by critical infrastructure.

Respondents to the open public consultation have rated the actual impact of an environmental damage caused by a cybersecurity incidents affecting products with digital elements as overall moderate. The average rating by all respondents was at 2.31 (on a scale of 1 to 5), with hardware and software manufacturers rating it at 1.82, users at 2.72 and consumer organisations at 5.

While the expected environmental impacts for neither of the policy options would be major, strengthening the cybersecurity of products with digital elements through policy option 4 having the widest scope of application, could have the most positive environmental impacts by contributing to wider use of latest generation of more sustainable digital infrastructure and services. This was confirmed in the targeted consultation, where respondents have indicated that option 4 is be expected to minimise environmental damage to the greatest extent[238], with the other options scoring lower[239].

7. HOW DO THE OPTIONS COMPARE?

Effectiveness: expected achievement of the objectives

As regards **effectiveness, options 3 and 4 featuring horizontal requirements** are more likely to meet the general and specific objectives set out in *section 4* compared to option 1 and 2, since they entail a regulatory horizontal intervention which would condition the placement on the market of certain or all products with digital elements to the compliance with essential cybersecurity requirements. This would ensure that security would be incorporated in the design and development of these products and that cybersecurity would become a baseline for products with digital elements placed on the internal market, with a high potential to improve the security of these products and also to improve the way users choose such products based on their cybersecurity.

Respondents to the open public consultation agreed that **horizontal requirements** would be the most effective measure, rating them with 4.08 on a scale from 1 to 5. Further voluntary European cybersecurity certification schemes for products with digital elements and services and EU public procurement guidelines taking into account cybersecurity requirements, as foreseen in policy option 1, were rated respectively at 2.99 out of 5, and 3.72 out of 5. Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances), as foreseen in policy option 2, rated overall 3.39 out of 5.

In terms of **security requirements**, 90.8% of the stakeholders agreed with the fact that hardware manufacturers and software developers should be responsible for the full life cycle of a product with digital elements. Stakeholders overall rated cybersecurity by design and by default as very effective approaches to contribute to the cybersecurity of products with digital elements, rating them respectively at 4.81 and 4.42 (out of 5, with 5 meaning very effective). Of these two horizontal regulatory options, policy option 4 would be more likely to meet these objectives compared to option 3, since it would also cover in its scope non-embedded software, hence ensuring a higher level of security for a wider scope of products, often dependent on each other.

[236] AXA (2020): "Environmental risks: cyber security and critical industries. An environmental white paper.", p. 1.
[237] Burk and Kallberg (2014): "The Forgotten Threat: The Environmental Consequences of Industrial Cyber Attacks", *American Water Resources Association Annual Water Resources Conference*.
[238] Score of 8.1 on a scale of 1 to 10.
[239] Option 3 at 6.6 and further down to option 0 at 3.1.

Furthermore **option 4 b)** would be more effective compared to option 4 a) as it would cover all non-embedded software, while in **option 4 a)** only critical software would be covered. **Option 4 b)** would also have a higher potential to ensure legal certainty and avoid further fragmentation of the internal market with regard to cybersecurity requirements applicable to products with digital elements. Keeping the status quo or relying on ad hoc regulatory interventions as regards cybersecurity or national voluntary schemes, as it would happen under policy options 1 and 2, would by contrast further deepen such fragmentation.

In terms of **scope**, stakeholders agreed with the effectiveness of applying cybersecurity requirements in the following way: hardware products (4.0 out of 5, with 5 indicating that they strongly agreed), embedded software (4.14 out of 5); all standalone software (3.7 out of 5); software products subject to higher cybersecurity risk (4.53 out of 5). While the effectiveness of covering standalone software was rated comparatively lower, this can be explained by a lower support from manufacturers (2.76 out of 5), while users still expressed a strong support (4.03 out of 5). The position of manufacturer is consistent with higher compliance costs linked to the coverage of all software products under policy option 4 b) (see 'efficiency' below).

In terms of conformity assessment, the **sub-option (ii)** establishing two risk categories informing conformity assessment under **policy option 3 and 4a) and b)** would respectively be more effective than options 3i), 4a)i) and 4b)ii) to enhance the security of products with digital elements. The involvement of a third-party body in the testing of higher risk products was broadly supported by stakeholders. 95.10% of the respondents in the public consultation supported the fact that products with digital elements with a higher risk should be subject to a stricter process of demonstrating conformity with these requirements. Only 2.92 (out of 5) agreed that self-declaration of conformity by a hardware manufacturer or software developer gives a sufficient confidence that security requirements are met. 86.15% agreed that involvement of a third party should be required under certain circumstances.

Considering the type of requirements, scope and conformity assessment procedures, policy option 4 b) ii) appears as most effective to reach the specific objectives set in *Section 4*.

Efficiency and economic impacts

Policy options 1 and 2 are likely to bring limited compliance costs, being mostly based on the use of voluntary measures. At the same time, the benefits would equally be limited as they would be mostly related to the reduction of legal uncertainty due to guidance (policy option 1) or the coverage of certain legislative gaps (policy option 2). Amending the RED delegated act to bring in all software would likely increase the benefits under policy option 2 close to policy option 3.

Policy options 3 and 4 would bring respectively significant economic benefits linked to the reduction of costs due to reduced cybersecurity incidents, estimated in the range of respectively EUR 90 to EUR 140 billion under policy option 3), EUR 97 to 158 billion under policy option 4 a) and EUR 180 to 290 billion under policy option 4 b). At the same time, compliance costs would be higher under policy option 3 and 4, compared to policy option 1 and 2. Under policy option 2, an exception is the scenario of broadening the scope of the RED delegated act to non-embedded software that would include higher compliance costs than under policy option 3 and 4 a).

The compliance costs for manufacturers and other economic operators on the supply chain would be triggered both by the design and development of products with digital elements with security as an inherent feature and the conformity assessment processes that go with that. These compliance costs increase with the scope and with mandatory third-party testing. Therefore, they are the highest under policy option 4) b) ii).

The table below presents the overview of all the economic impacts analysed in this report. Concerning the methodology for the comparison of impacts, the report generally operates with

the "+/-" rating system for impacts that were qualitatively assessed. To the extent possible, were quantitative data was available, the net impact and cost-benefit ratio has been estimated.

The table evidences the **net positive impact** increasing with a broadened scope between policy option 3 and 4. The net positive impact is the highest for policy option 4 and its respective sub-options. While no granular quantitative data is available, it is reasonable to assume that the net positive impact would be the highest for policy option 4b) ii).

It is not possible to define a detailed **cost-benefit ratio comparison** of sub-options. The cost-benefit ratio which is higher for policy option 3 compared to 4 can be explained by the absence of granular quantitative data for benefits at the level of sub-options. While the benefits "only" double between policy option 3 and 4, the compliance costs increase more significantly as software products have lower BaU costs, e.g. for testing. Furthermore, the software market is slightly bigger compared to the hardware market[240]. At the same time, benefits in terms of reduction of cyber incidents, competitiveness and prevention of internal market fragmentation increase with a broadened scope, and are expected to be the highest under policy option 4) b) ii).

Under options 3 to 4 and their respective sub-options, the effects of additional compliance costs will have a larger relative cost impact on **SMEs** than on large companies. Such compliance costs would be the highest under policy option 4 b) ii). Even though the relative cost increases are higher for SMEs, the impact on SMEs overall costs is still considered moderate when measured against the benefits that would result from a reduced number of cybersecurity incidents that would be most significant under policy option 4 b) ii). SMEs rated the costs of voluntary measures in average at 3.1 out of 5 (with 5 indicating very costly), compared to 3.6 for policy option 2, and around 3.5 out of 5 for horizontal requirements.

For **Member States and public authorities**, the direct costs would increase with a broader scope of products to be monitored, hence the direct costs would be the highest under **policy option 4 b)**. For the same scope, enforcement costs are expected to be higher without third party-assessment, under policy option 3 i) and 4a)i) and 4b)i) compared to 3 ii) and 4 a)ii) and 4b)ii). Public authorities will benefit under policy option 3 and 4 as users of products with digital elements from an enhanced security of products and reduced costs due to less cybersecurity incidents. Market surveillance authorities could also benefit in terms of efficiency from alignment of the provisions for market surveillance for harmonised and non-harmonised products with digital elements. Such benefits are expected to be the highest under policy option 4 b) ii).

Consumers will benefit from the reduction of unsecure products with digital elements on the market. The trend of the impact of the different options on the reduction of costs due to cybersecurity incidents can be reasonably assumed to be similar as for businesses. Hence, they can expected to be the highest under policy option 4 b) ii). Consumers might face higher end-user prices on products with digital elements, which can be expected to be the highest under option 4 b) ii). However, these are not expected to be significant both in terms of quantitative and qualitative value to the consumers and will decrease over time (see *section 6.3.4*).

[240] Hardware products represent 48% of the relevant market, compared to 52% for the software market.

	Key Costs/benefits	Policy options							
		PO 1	**PO 2**	**PO 3**		**PO 4**			
				3 (i)	3 (ii)	4a)		4b)	
						4a) i)	4a)i)	4b)i)	4b)ii)
	Businesses								
Costs	Compliance costs (for average product development cost of 140 000 EUR)	*Neutral/+*[241]	+/++[242]	**EUR 11.2 bn**	**EUR 11.3 bn**	**13 bn EUR**	**13.1 bn EUR**	**EUR 28.8 bn**	**EUR 29 bn**
	Compliance costs for SMEs [243]	+	++	++	++	++	++	+++	+++
	Standardisation costs	*Neutral*	++	+	+	++	++	+++	+++
	End-user prices (indirect)	*Neutral/+*	*Neutral/+*	+	+	++	++	+++	+++
Benefits	Cost savings due to reduced cyber incidents	*Neutral*	+	**EUR 90 billion to EUR 140 bn annually**		**EUR 97 bn to EUR 158 bn**		**EUR 180 to 290 bn annually**	

[241] Due to the voluntary nature, compliance costs to be compensated by benefits. However, compliance costs can occur through an indirect market pressure in case of uptake of voluntary measures by the demand side (public procurement guidelines, EU certification).

[242] Additional compliance costs depending on sectoral legislation, possibly high in the case of amendment of RED to include standalone software.

[243] Based on feedback received in open public consultation: SMEs rated the costs of voluntary measures in average at 3.1 out of 5 (with 5 indicating very costly), compared to 3.6 for policy option 2, and around 3.5 out of 5 for horizontal requirements respectivel on software and hardware.

	Prevent internal market fragmentation[244]	*Neutral/ -*	*Neutral / -*	+	+	++	++	+++	+++
	Increased competitiveness & uptake of products with digital elements	*Neutral*	*Neutral*	+	+	++	++	+++	+++
	Net value*				**EUR 77.8 - 127.8 bn**		**EUR 93 bn - 144.9 bn EUR**		**EUR 151- 261 bn**
	Cost benefit ratio*				**7.4 - 11.5**		**7.4 - 12.1**		**6.2 - 10**
	Public authorities								
Benefits	Reduced cyber incidents	*Neutral*	+	++	++	++/+++	++/+++	+++	+++
Costs	MS authorities - enforcement costs (average for products on the market)	*Neutral/+*[245]	*++*[246]	**EUR 3.1 bn**	**EUR 3.1 bn**	**EUR 3.6 bn**	**EUR 3.6 bn**	**EUR 7.7 bn**	**EUR 7.7 bn**
	ENISA - collecting and disseminating information on exploited vulnerabilites	*N.A.*	*N.A.*	**2.5 FTEs**	**2.5 FTEs**	**3.5 FTEs**	**3.5 FTEs**	**4.5 FTEs**	**4.5 FTEs**

[244] Based on responses from open public consultation

[245] Additional costs for market surveillance authorities if a new EU certification scheme is implemented. For voluntary measures, like guidelines, no costs expected.

[246] Additional enforcement and adjustement costs for MSAs due to addition of cybersecurity requirements, and possibly standalone software

	(redistribution of ressources)								
	Consumers								
Benefits	Reduced cyber incidents	*Neutral*	+	++	++	++/+++	++/+++	+++	+++
	Enhanced consumer choice & transparency[247]	+	+	++	++	++	++	+++	+++
Costs	End-user prices (indirect)	*Neutral/+*	*Neutral/+*	+	+	++	++	+++	+++

***** based on available quantitative data*

Table 9: Comparison of policy options according to the economic impact and efficiency

[247] based on feedback from the open public consultation

Social impacts, impacts on fundamental rights and environmental impacts

As regards the **social impact,** as well as the impact of **fundamental rights**, and notably data protection and protection of privacy, it is expected that policy options 3 and 4 would have a more positive impact, as attacks affecting insecure products with digital elements have serious consequences in the personal sphere and for society as a whole. Therefore, these two policy options, which would ensure a higher level of cybersecurity for these products, would be more impactful on fundamental rights and social aspects. Since policy option 4 a) and b) would cover also standalone software, considering the importance of such products (such as apps) for social aspects and personal data, it would be expected that the positive impact would be the highest for policy option b). Furthermore, third-party assessment would increase the assurance level of the security of higher risk hardware and software products, hence the social impact and impact on fundamental rights would be the highest for policy option 4 b) ii).

No major **environmental** impact is expected for any of the policy options considered. However, strengthening the cybersecurity of products with digital elements notably through policy option 4 which would have the widest scope of application could have positive environmental impacts by contributing to wider use of latest generation digital infrastructure and services, which are more sustainable.

Coherence

As regards the coherence with the **EU strategic policy priorities in the area of cybersecurity**, policy options 3 and 4 would deliver the most on the establishment of common European cybersecurity standards for connected products as forseen under the EU's Cybersecurity Strategy for the Digital Decade[248]. Policy option 4 b), presenting the widest scope and covering all products with digital elements, would be the most aligned with the announced objective.

Regarding other **horizontal EU legislation in the area of cybersecurity**, both **policy 3 and 4** would present strong synergies with the supply chain security requirements included in the **NIS2 Directive**, now close to completing adoption. Entities under NIS2 will have to consider the vulnerabilities specific to each direct supplies (such as of software for example) and the overall quality of products and cybersecurity practices of their suppliers, including development procedures. Horizontal requirements for all products with digital elements, including third-party assessment for higher risk products, as foreseen under **policy option 4 b) ii)**, would strengthen this provision most and close the circle of supply chain security guarantees.

Regarding the **EU Cybersecurity Act**, policy option 1 would be the most coherent as it foresees to continue developing such schemes. However, both under policy option 3 and 4, a certificate or statement of conformity issued under an European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.

As regards the coherence **with other relevant product legislation**, both policy options 3 and 4 and respective sub-options, would include specific cybersecurity requirements of the likes that are not currently covered by the NLF legislation. Furthermore, the act setting out the horizontal cybersecurity requirements would set out a rule of the type of *lex specialis,* specifying that where, for a certain category of products with digital elements, the cybersecurity risks addressed by the essential requirements are covered by other more specific requirements of other Union harmonization legislation, these

[248] JOIN(2020) 18 final.

horizontal requirements shall not apply to those products to the extent that that specific Union legislation covers such risks.

As regards the RED Delegated Regulation for inter-connected radio equipment, it would be implemented until the horizontal requirements start applying. As the horizontal requirements would be more specific, the RED Delegated act requirements would become obsolete. Alternatively, compliance with the horizontal cybersecurity requirements could be presumed to provide compliance with the cybersecurity requirements of RED delegated act. Moreover, when preparing the standardisation request for the horizontal cybersecurity requirements, it will be ensured that the standardisation work done for the RED Delegated Regulation is preserved and complemented only where needed.

When it comes to the coverage of the whole life cycle and duty of care, policy options 3 i) and ii) and 4 a) and b) would be compatible with the future EU framework on liability for defective products, to be reviewed, which is expected to introduce liability for situations when damages are triggered by vulnerabilities. The liability of an economic operator may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person [including, for example, rejecting a software security update] or any person for whom the injured person is responsible.

Proportionality

As regards the **proportionality of the intervention**, policy options 3, 4 a) and b) do not go beyond what is necessary to meet the specific objectives satisfactorily. Any additional compliance costs would be outweighed by the benefits brought by a higher level of security of products with digital elements and ultimately an increase of trust of users in these products. For these reasons, but also for the need to ensure legal certainty and avoid any further fragmentation of product-related requirements on cybersecurity on the internal market, the open public consultation and the targeted consultation have shown a wide overall **support of various stakeholders**, both industry and national authorities for a horizontal intervention setting out cybersecurity requirements for products with digital elements.

Stakeholder support

In the public consultation, respondents were asked to rate the effectiveness of various types of policy interventions ranging from further voluntary certification schemes and amending existing legislation regulating specific products to mandatory horizontal cybersecurity requirements for hardware and software. Respondents agreed that **horizontal requirements for hardware and software would be the most effective measure**, and rated it respectively 4.08 and 4.09 on a scale from 1 to 5. This includes consumer organisations (5.00), respondents identifying themselves as users (4.22), notified bodies (4.17), MSAs (5.00) and manufacturers of products with digital elements (3.85), as well as SME users and manufacturers (4.05). The other types of interventions were rated as follows:

- Further voluntary European cybersecurity certification schemes for products with digital elements and services: overall (2.99), national market surveillance bodies (2.0), consumer associations (1.3), public administrations as users (2.9), SMEs as users (3.2), hardware manufacturers (2.5), software manufacturers (3.4), SMEs in their role as manufacturers (2.7).
- EU public procurement guidelines taking into account cybersecurity requirements: overall (3.72), national market surveillance bodies (2.5), consumer

associations (2.3), public administrations as users (4.1), SMEs as users (4.2), hardware manufacturers (3.3), software manufacturers (4.1), SMEs in their role as manufacturers (3.7).

- Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances): overall (3.39), national market surveillance bodies (3.5), consumer associations (3.0), public administrations as users (4.5), SMEs as users (3.5), hardware manufacturers (2.2), software manufacturers (3.3), SMEs in their role as manufacturers (2.1).

There are several reasons why policy option 4 is broadly supported by the manufacturers of products with digital elements despite the relatively high cost compared with other types of intervention. First of all, the security of products with digital elements also depends on the security of components integrated into those products. Manufacturers therefore have to rely on their upstream supply chain manufacturers taking security seriously. A horizontal intervention would ensure that manufacturers could integrate components developed to meet certain security requirements. Secondly, a horizontal intervention would provide manufacturers with a high degree of legal certainty, as it would do away with the current piecemeal approach of Union NLF product legislation when it comes to cybersecurity. Finally, under a horizontal intervention, higher costs related to cybersecurity would no longer translate into a competitive disadvantage for manufacturers, as their direct competitors would be required to develop products living up to the same high standards. As stressed under 'efficiency', there is nevertheless a concern by manufacturer regarding the compliance costs related to the inclusion of all non-embedded software into the scope of a possible horizontal initiative (as foreseen under option 4b). On the contrary, such an approach is strongly supported by users.

Overview and overall assessment of all policy options

The table below presents a simplified overview of negative and positive impacts by type of impact.

Impacts	Option 0 *Status quo*	Option 1 *Soft law*	Option 2 *Ad-hoc interv.*	Option 3 *Mixed approach*		Option 4 *Horiz. Interv.*	
				3 i)	3 ii)	4 a)	4 b)
						4 a) i)	4 b) ii)
Effectiveness							
Economic/Efficiency							
Environmental							
Social							
Fundamental rights							
Coherence							
Stakeholder support							
Proportionality							
Total							

The symbols ■ and ■ indicate respectively positive and negative impacts as compared to the status quo. For each symbol a maximum scale of 1 to 3 (maximum positive or negative assessment) is used.

Table 10: Overall impact of the various policy options

While **Option 1** is causing no major additional costs for businesses and MSAs, it is unlikely to be adequate to address the problems identified. While legal uncertainty will be slightly reduced due to Commission guidance, it will not have the effect to significantly changing security market practices. Option 1 is also expected to deepen market fragmentation in the absence of horizontal cybersecurity requirements.

Option 2 is causing limited compliance costs except under the scenario where the RED delegated act would be extended to include all software, where compliance costs would be high (for economic operators and MSAs). Option 2 would only partially adequately address the identified problems, as gaps will remain regarding the coverage of hardware (e.g. wired hardware). Furthermore, option 2 could also have the effect of deepening market fragmentation by taking a product-specific approach instead of introducing horizontal requirements.

Option 3 is linked to somewhat higher additional compliance costs, however lower than Option 2 (under the scenario of amending RED delegated act). Horizontal requirements for hardware and software received strong stakeholder support. Both under 3i) and 3ii) horizontal requirements would avoid market fragmentation for hardware products and embedded software. While compliance costs would slightly increase under option 3ii), mandatory third-party assessment for higher risk products would be even more effective to enhance cybersecurity, and ease market surveillance. However, under option 3, a significant gap would remain for enhancing cybersecurity of and preventing market fragmentation for non-embedded software products.

Option 4 would lead to higher costs for businesses and market surveillance authorities, while such costs would be lower under option 4 a) if only critical software is covered, compared to option 4 b). Option 4a) including third-party assessment received strong stakeholder support. Most stakeholders disagreed that self-assessment could be sufficient. However, option 4 a)ii) would again leave a gap for a large part of the software market (estimated at 90%).

Option 4 b) including third-party assessment would bring the most significant compliance costs. It was nevertheless strongly supported by stakeholders. The compliance costs would be proportionate to the significant cost savings that can be drawn from reduced cybersecurity incidents and from having to comply with multiple product-specific cybersecurity requirements. Under option 4 b)ii) mandatory third-party assessment for higher risk products would be even more effective to enhance trust of users, and ease market surveillance, while higher compliance costs would be limited to a narrow category of products presenting a higher risk.

8. PREFERRED OPTION

8.1. Rationale and benefits of the preferred option

Policy option 4 sub-option b) ii) emerges as the preferred option based on the assessment of effectiveness against the specific objectives and efficiency of costs versus benefits, and coherence with the existing EU and policy framework. The option would deliver the best results, while compensating higher compliance costs with significant cost savings. It

would have the highest compliance costs, both for businesses and MSAs and slightly higher prices for end-users. However, it would also bring the highest benefits in terms of costs savings due to the reduction of cybersecurity incidents and harmonised cybersecurity requirements. Furthermore, additional compliance costs for conformity assessment would only apply to a limited category of products justified on the basis of their higher risk.

Option 4 b) would ensure the setting out of specific horizontal cybersecurity requirements for all products with digital elements being placed, made available in the internal market, and would be the only option covering the entire digital supply chain. Standalone software, equally exposed to vulnerabilities, would also be covered by such regulatory intervention, thus ensuring a coherent approach towards all products with digital elements, with a clear share of responsibilities of various economic operators. This would ensure a design and development of products with digital elements that would have cybersecurity as an ingrained feature, while at the same time guaranteeing a proportionate approach that would avoid unnecessary burden on manufacturers and the other economic operators on the value chain. The security requirements set out would be objective-oriented and not product- or sector-specific, while at the same time ensuring sufficient granularity to generate a tangible impact on the level of cybersecurity of products with digital elements.

As regards the way in which manufacturers would be able to demonstrate conformity with the security requirements, sub-option (ii) emerges as the preferred choice: two risk categories informing self-assessment (by default), third-party conformity assessment (for critical products). Sub-option (ii) is proportionate, as the vast majority of products with digital elements would be subject to self-assessment, which is generally associated with the lowest administrative burden and compliance costs for manufacturers. At the same time, it would also be effective in ensuring an adequate level of assurance for a small number of products carrying a higher risk, by subjecting these products to mandatory third-party conformity assessment.

This policy option also brings added value by covering duty of care and whole life cycle aspects after the placement of the products with digital elements on the market, to ensure, among others, appropriate information on security support and provision of security updates.

This policy option would also come to most effectively complement the recent review of the NIS framework, by ensuring the prerequisites for a strengthened supply chain security.

8.2. Application of the ‘one in, one out’ approach

"INs": administrative costs related to third-party assessment (certification), documentation and reporting

The preferred option is likely to lead to an increase of compliance costs for businesses. The total market affected is detailed in section 5.1, and would represent a total turnover of up to EUR 1 485 billion and 615 272 companies/products (see also *Annex 3*). First, hardware and software manufacturers will be impacted by adjustment costs as a result of the new and additional cybersecurity requirements and internal testing costs. And secondly, conformity assessment procedures involving a third-party when placing products on the market and documentation requirements will lead to additional administrative costs. These adjustment and administrative costs and the methodology behind them are explained in detail in section 6, including the limitations behind these quantitative estimates.

In total, it is estimated that this initiative would lead to **additional administrative costs of approximately EUR 8.9 billion** for the whole of the EU ('IN'), taking into account BaU costs. **The one-off administrative costs would amount to EUR 7.6 billion, with recurrent costs of EUR 1.3 billion.** These costs have to be put into perspective with the administrative savings linked to this initiative ('OUT') detailed below.

The administrative costs under the preferred option are estimated under *section 6*, and summarised in *table 7*. They include the costs related to certification that would apply to 10% of the market (estimated share of critical products with digital elements, estimated at EUR 1.1 bn, or 25 000 EUR by company/product with BaU costs at 40% for hardware manufacturers and 25% for software manufacturers, see *Annex 4*) and costs related to conformity other than certification (EUR 7.8 bn, or 12 600 EUR by company/product). The impacted market is represented by the indicators SD and ICT-EXT-ADJ. Furthermore, the assumption is taken of one product by company and an average product development cost of 140 000 EUR.

In order to distinguish between **one-off and recurrent costs**, regarding the third-party assessment costs, at a level of a company, for each new product that has to be tested the one-off costs will be higher than recurrent costs, therefore it is assumed that 70% of the costs represent one-off costs (e.g. auditing and reviewing of documentation by external party and fees to notified body) and that 30% represent recurrent costs related to the maintenance of the certification (e.g. regular audit for the maintenance of the certification). However, this differentiation of one-off and recurrent costs could not be corroborated by secondary or primary data.

Regarding other types of administrative costs, including documentation and reporting, no granular data is available. For documentation and information obligations, it is estimated that the one-off costs would be slightly higher (linked to the creation of the documentation), while recurrent costs would still exist due to the obligation for the manufacturer to keep its documentation up to date and to provide information to the users throughout the lifecycle. A significant part of the other types of administrative costs could be linked to reporting obligations. The costs of reporting obligations would be both one-off (e.g. putting in place a reporting system) and recurrent. Based on the primary data gathered[249], it is assumed that the documentation and reporting obligations would respectively represent 60% and 40% of the total costs. Furthermore, both for documentation and reporting obligations, one-off costs would be higher than recurrent costs, and can be estimated respectively around 12.5%[250] based on the same primary data.

In detail, the administrative costs related to documentation and reporting can be described as follows:

- Requirements related to the declaration of conformity and marking of the digital products
    - Where compliance of the product with the applicable requirements has been demonstrated by that procedure, draw up an EU declaration of conformity and affix the CE marking.
    - Keep the EU declaration of conformity up-to-date.

[249] Targeted survey on impacts launched on 16 May 2022 organised by the study supporting this impact assessment. As mentioned in section 6, this data could not be verified and has been used in the absence of secondary data.
[250] Targeted survey on impacts launched on 16 May 2022: in the responses, stakeholders indicated ranges between 1% and 25%.

    - Ensure that each digital product is accompanied by a copy of the EU declaration of conformity.
    - Keep the EU declaration of conformity for 10 years after the product has been placed on the market.
    - Keep a register of complaints, non-conforming products and product recall, and keep distributors informed of any such monitoring.
    - Ensure that products bear a type, batch or serial number or other element allowing their identification, or, where the size or nature of the product does not allow it, that the required information is provided on the packaging or in a document accompanying the product.
    - Indicate the manufacturers' name, registered trade name or registered trademark, and the address at which they can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product.
- Requirements related to reporting of the digital products
    - Report to ENISA exploited vulnerabilities and incidents having an impact on the security of the product with digital elements.
    - Inform the user about any incident having an impact on the security of the product with digital elements.
    - Immediately inform the relevant national competent authority should the product present cybersecurity risks that pose threats to the general public or the life and health of persons.
    - Upon identifying a vulnerability in an open-source component and where the manufacturer or developer has integrated the component into its product, report the vulnerability to the maintainer of the component.
    - Further to a reasoned request from a competent national authority, provide it with all the information and documentation necessary to demonstrate the conformity of the product, in a language, which can be easily understood by that authority. Cooperate with that authority, at its request, on any action taken to eliminate cybersecurity risks posed by the product, which they have placed on the market.
- Requirements related to technical documentation of the digital products
    - Draw up the necessary technical documentation before the product is placed on the market in a language that is accepted by the notified body.
    - Keep the technical documentation up-to-date.
    - Keep the technical documentation for 10 years after the product has been placed on the market.
    - Make the technical documentation available to authorities upon request.

The table below summarises the administrative costs related to certification, documentation and reporting for one company/product, and at aggregated level. The costs are based on the products currently available on the market (using the SD and ICT-EXT-ADJ indicators), as it is not possible to estimate how many products will arrive on the market every year. In practice, the new obligations under the preferred option would only apply after a transition period to new products placed on the market (grandfathering clause). The recurent costs are assumed to be annual. These estimations were made based on limited quantitative data available. Therefore, the first evaluation of this initiative (see *Section* 9) should explore a more granular assessment of the administrative costs on businesses.

Per company	One-off costs	Recurrent costs (annual)	Total
Administrative costs linked to testing			
Certification for critical products (third-party conformity assessment)	• By company/product: EUR 17 500 • Aggregated costs: EUR 0.8 bn (70% of the costs are audit cost by the notified body to obtain the certification)	• By company/product: EUR 7 500 • Aggregated costs: EUR 0.3 bn (30% are related to monitoring the certification,)	• Average by company/product 25 000 EUR (with BaU costs of 40% for hardware manufacturers and 25% for software developers) • Aggregated: **EUR 1.1 bn**
Other administrative costs : documentation and reporting			
Documentation, such as creation and updating of technical documentation, EU declaration of conformity; affixing the CE marking; Creation of and updating the risk assessment; Information and instructions for the user, including when providing software updates.	• By company/product: 6615 • Aggregated costs: EUR 4.1 bn	• By company/product: 945 EUR • Aggregated costs: EUR 0.6 bn	• **by company/product: 9% of product development costs** (in average additional EUR 12 600, of which EUR 7560 documentation and 5040 reporting costs, for average product development costs of 140 000 EUR) • Aggregated: **EUR 7.8 bn** (of which EUR 4.7 bn for documentation and EUR 3.1 bn for reporting)
Reporting to market surveillance authorities Reporting of exploited vulnerabilities and cybersecurity incidents to ENISA	• By company/product: EUR 4410 • Aggregated costs: EUR 2.7 bn	• By company/product: EUR 630 • Aggregated costs: EUR 0.4 bn	
TOTAL	• By company/product (in average): EUR 25 060 (for average development costs of 140 000 EUR, ca. 17% additional product development costs) • Aggregated average: **EUR 7.6 bn**	• By company (in average): EUR 12 540 for average development costs of 140 000 EUR, ca. 9% additional product development costs) • Aggregated average: **EUR 1.3 bn**	• by company/product covered by the initiative: EUR 37 600, ca. 26% additional product development costs, for an average of 140

			000 product development costs. • Aggregated: **8.9 bn EUR**

Table 11: Overview of one-off and recurrent administrative costs

"OUTs": administrative savings due to reduced compliance costs with the upcoming NIS2 Directive

The administrative costs should be offset with **removed administrative costs** linked to the initiative. In total, these administrative cost savings are estimated to represent approximately **EUR 6.95 billion**. Administrative costs savings are related to two main sources. First, the initiative will facilitate compliance with administrative costs related to supply chain managamenet under the upcoming NIS2 Directive. Second, the initiative will prevent fragmented rules at national and EU level related to the cybersecurity of products with digital elements. Only the first source of potential administrative savings could be quantified.

Under the upcoming NIS2 Directive[251], entities must take cybersecurity risk management measures, including measures to secure their supply chains. The approximately 110 000 entities in the scope of NIS2 would therefore experience significant cost savings brought about by the preferred policy option, which would enhance the security of the products with digital elements used in the whole supply chain[252]. Supply chain requirements under NIS2 would for instance include managing the contractual relationships with suppliers and auditing suppliers to verify that purchased products comply with the cybersecurity requirements. In the context of the Impact Assessment of the NIS2 Directive, the costs related to **"Security elements concerning supplier relationships and supplier-specific risk assessment**" where estimated as one-off costs of hiring in average **1 FTE by company** , and a potential increase of **2-4% in recurrent purchase ICT security costs**. One FTE position can be estimated at a cost of EUR 66 560[253], which would represent EUR 7.3 billion one-off costs for the 110 000 entities covered by NIS2. According to the Commission's impact assessment for the revision of the NIS Directive, the average ICT security spending of companies in 2020 is of approximately 9.14 % of their ICT spending.[254] According to an ENISA survey[255], the median spending of an entity covered by NIS for IT security spending was EUR 2 million per entity in 2020, which leads to an aggregated value of EUR 220 billion, of which 2-4% (taking an average of 3%) would amount to EUR 6.6 billion recurrent costs.

Taking into account that the initiative will not apply directly to IT services[256], it is assumed that the initiative would lead to **50% of compliance cost reduction** with the requirement related to supply chain security for essential and important entities. Hence,

[251] The entry into force of the NIS2 Directive is planned 21 months after its publication in the Official Journal. A political agreement on the NIS2 Directive was reached in May 2022.
[252] See Article 21.2 (d) the compromise text of the NIS2 Directive from 17 June 2022: "(d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers".
[253] With following assumptions: 40 hours per week x 52 weeks per year = 2,080 hours ; hourly wage of 32 Euros (See *Impact Assessment* for AI Act)
[254] SWD(2020) 345 final, IA accompanying the NIS2 proposal, p. 71.
[255] https://www.enisa.europa.eu/publications/nis-investments-2021
[256] According to the study "The Economic and Social Impact of Software & Services on Competitiveness and Innovation" (SMART 2015/0015) prepared for the European Commission, cloud computing represented 18.3% of the software market in 2020, and infrastructure and application-related IT services respectively 21.2% and 29.3%.

the cost savings would respectively represent in total **EUR 6.95 billion**, **with EUR 3.65 billion from one-off costs and EUR 3.3 billion recurrent costs**.

Cost savings	One-off cost savings	Recurrent cost savings
Costs savings on compliance with NIS2 obligations (supply chain security requirement for essential and important entities)	• By company: 0.5 FTE (in average: EUR 33 280) for NIS entities • Aggregated average: EUR 3.65 bn	• By company: 1-2% additional ICT security spending, for NIS entities (around 30 000 EUR by company, taking an average of 1.5%) • Aggegrated average: EUR 3.3 bn
Administrative costs	• Aggregated average: EUR 7.6 bn	• Aggregated average: EUR 1.3 bn
Total Administrative burden *(administrative costs minus cost savings)*	• Aggregated: EUR 3.95 bn	• Aggregated: - EUR 2 bn

Table 12: Overview of cost savings and total administrative burden

Moreover, cost savings would stem from hvaing one horizontal framework. Tnstead of potentially conflicting rules at national level or a piecemeal approach at EU level, the preferred option is likely to offset compliance costs by introducing one set of streamlined requirements for the same type of product with digital elements at EU level, which would reduce regulatory costs for the manufacturers. Indeed, most stakeholders favour a harmonised and coordinated approach at the EU level as revealed in the open public consultation, targeted survey, workshops and interviews. However, the costs related to streamlining security requirements could not be estimated.

Taking into account on the one side, the administrative costs related to the initiative under the preferred policy option and on the other side, the administrative savings, the **total administrative burden of the preferred option for businesses operating in Europe**[257] would be of approximately **EUR 1.95 billion**, for an overall market value covered by the initiative of up to EUR 1317 billion in production value and EUR 1485 billion in turnover (based on 2019).

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

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. The report shall be made public. The application of the regulation should in principle be set for approximately 24 months following its entry into force, to allow sufficient time to the economic operators to adapt and prepare adequate implementation.

As regards the monitoring of the impact of the regulation, certain indicators would be considered for this purpose, to be assessed by the Commission, where appropriate with the support of ENISA. Depending on the operational objective to be reached, some of the

[257] This report cannot distinguish between EU and non-EU businesses.

monitoring indicators based on which the success of the horizontal cybersecurity requirements would be assessed are as follows:

A. For assessing the **level of cybersecurity of products with digital elements**:
   - ✓ Statistics and qualitative analysis on incidents affecting products with digital elements and the way these were handled. These could be gathered and assessed by the Commission and be based on the information reported to ENISA.
   - ✓ Records of known vulnerabilities and analyses of how these were handled. Such analysis could be conducted by ENISA, based on the European vulnerability database set up based on NIS2 and information reported to ENISA under this initiative.
   - ✓ Surveys amongst manufacturers of hardware and software to monitor progress.

B. For assessing the **level of information on security features, security support, end-of-life and duty of care**: results of surveys to be conducted by the Commission, with support from ENISA for both consumers and businesses.

C. For assessing the implementation, the Commission would aim to ensure that the **conformity assessments are effectively performed**. To this end, the coordination of notified bodies will be promoted. Furthermore a standardization request could be issued and its implementation followed. The Commission will also verify the capacity of the notified bodies.

D. As regards the **application**, by means of the reports of Member States, the Commission will verify that national initiatives do not concern aspects covered by the regulation.

The following table lists provisional and non-exhaustive indicators, indicating how meeting the set general and specific objectives can be measured.

Specific objective	***Indicator***	***Baseline***	***Frequency***	***Target***	***Source***
Ensure that manufacturers improve the security of their products with digital elements since the design and development phase and throughout the whole life cycle of those products	*Number of serious incidents in the Union resulting from vulnerabilities in products with digital elements*	*2024*	*Annual*	*Reduction of incidents by roughly 20 to 33 % (difficult to measure as other developments may influence the outcome)*	*Aggregate incident reporting mechanism under the NIS2*
	Share of hardware and software manufacturers that follow a systematic secure development life cycle	*2024*	*Biennial*	*100 %*	*Surveys amongst hardware and software manufacturers*
	Qualitative analysis of the security of	*2024*	*Biennial*	*n/a*	*ENISA, surveys amongst security experts*

	products with digital elements				
	Maturity of secure development practices in manufacturers: *—quantitative and qualitative assessment of vulnerability databases;* *—frequency of security patches made available by manufacturers;* *—average number of days between vulnerability discovery and the provision of security patches*	*2024*	*Biennial*	*—Reduction of vulnerabilities by 20 to 33 % (difficult to measure as other developments may influence the outcome)* *—Higher frequency of patches* *—Shorter average number of days between vulnerability discovery and the provision of security patches*	*ENISA, market surveillance, surveys amongst security experts, European vulnerabilities database set up on the basis of NIS2, cybersecurity studies*
Ensure a coherent cybersecurity framework	*Absence of targeted product-specific national cybersecurity legislation*	*2024*	*Biennial*	*Absence of targeted product-specific national cybersecurity legislation*	*Surveys, studies, TRIS notification procedure under Directive 2015/1535*
Enhance the transparency as regards the security properties of products with digital elements	*Share of products with digital elements that are shipped with information on security properties*	*2024*	*Biennial*	*100 % of products with digital elements shipped with information on security properties*	*ENISA, market surveillance bodies, studies*
Enable organisations and consumers to use products with digital elements securely	*Share of products with digital elements that are shipped with user instructions on secure use*	*2024*	*Biennial*	*100 % of products with digital elements shipped with user instructions on secure use*	*ENISA, market surveillance bodies, studies*

Table 13: Indicators for monitoring and evaluation

GLOSSARY OF ABBREVIATIONS

Acronym	Meaning
AI	Artificial Intelligence
B2B	Business to Business
B2C	Business to Customer
BaU	Business as Usual
CAGR	Compound Annual Growth Rate
CLA	Cybersecurity Labelling Scheme
CN	Combined Nomenclature
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CSD	Consumer Sales Directive
CSIRTs	Cyber Security Response Teams
DDoS	Distributed Denial of Service
DoC	Declaration of Conformity
DoP	Declaration of Performance
eIDAS (Regulation)	Regulation on electronic identification and trust services for electronic transactions in the internal market
ENISA	European Union Agency for Cybersecurity
EO	Executive Order (US)
FTE	Full Time Equivalent
GDPR	General Data Protection Regulation
GPSD	General Product Safety Directive
GPSR	General Product Safety Regulation (proposal)
IA	Impact Assessment
IaaS	Infrastructure as a service (cloud service model)
ICS	Industrial Control System
ICT-SC	ICT – standard classification
IoT	Internet of Things
METI	Ministry of Economy, Trade and Industry of Japan
MDR	Medical Devices Regulation
MID	Measuring Instrument Directive
MR proposal	Machinery Regulation Proposal
MSA	Market Surveillance Authority

MSD	Market Surveillance Services Directive
MSR	Market Surveillance Regulation
NIS (Directive)	Directive concerning measures for a high common level of security of network and information systems across the Union
NIST	National Institute of Standards and Technology – US Department of Commerce
NLF	New Legislative Framework
NTIA	National Telecommunications and Information Administration (US)
OSS	Open Source Software
OT	Operational Technology
OWASP	Open Web Application Security Project
PaaS	Platform as a service (cloud service model)
PED	Pressure Equipment Directive
RED	Radio Equipment Directive
RRD	Recreational Craft and Personal Watercraft Directive
SaaS	Software as a Service (cloud service model)
SBOM	Software Bill of Materials
SDLC	Secure Development Life Cycle
SMEs	Small and Medium-sized Enterprises
SOCs	Security Operation Centres
TFEU	Treaty on the Functioning of the European Union
TSD	Toy Safety Directive

GLOSSARY OF TERMS AND DEFINITIONS

Term	Meaning or definition
Ancillary service	A digital service the absence of which would prevent the product [tangible and intangible] from performing one of its functions
CE marking	The letters 'CE' appear on many products traded on the extended Single Market in the European Economic Area (EEA). They signify that products sold in the EEA have been assessed to meet high safety, health, and environmental protection requirements.
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements, following certain procedures.
Conformity assessment	The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled (point (12) of Article 2 of Regulation (EC) No 765/2008).
Conformity self-assessment	A conformity assessment performed by the manufacturer without third party involvement. The manufacturer himself or an accredited in-house conformity assessment body that forms a part of the manufacturer's organization, carries out all required controls and checks, establishes the technical documentation and ensures the conformity of the production process.
Cybersecurity	The activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats
Product with digital elements	Hardware and software products which can be directly or indirectly connected to another device or network, as follows: ➢ any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data.[258] *E.g. end devices such as: laptops, smartphones, sensors and cameras; smart robots; smart cards; smart meters; mobile devices; smart speakers or networks, such as: routers; switches.* ➢ embedded software: Firmware or other software that is essential for the primary function of the end-product and is either: (i) pre-installed in a product; or (ii) separately placed on the market by the manufacturer and downloaded to a product at a later stage. *E.g. firmware, basic operating systems; network system; storage and security management.* ➢ non-embedded software ('standalone' software): Software that is additional to the primary function of the device on which it is downloaded.[259] *E.g. extended operating system, mobile apps.*
Distributed denial-of service (DDoS) attack	A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.
End of life (of a product with digital elements)	The state of a product having reached the end of its first use until its final disposal.

[258] NIS2 Directive proposal, Article 4(1)(b).
[259] The distinction is in the function of the software: it adds to the basic functionality of the device on which it is downloaded.

European cybersecurity certification scheme	According to the *EU Cybersecurity Act,* it means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.
Intended purpose	The use for which a product with digital elements is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation
Life cycle (of a product with digital elements)	Consecutive and interlinked stages of a product from first use to final disposal.
New Legislative Framework (NLF)	A framework built on Regulation (EC) No 765/2008 and Decision No 768/2008/EC bringing together all the elements required for a comprehensive regulatory framework to operate effectively for the safety and compliance of industrial products with the requirements adopted to protect the various public interests and for the proper functioning of the single market. The new legislative framework was adopted to improve the internal market for goods and strengthen the conditions for placing a wide range of products on the EU market. It is a package of measures that streamline the obligations of manufacturers, authorised representatives, importers and distributors, improve market surveillance and boost the quality of conformity assessments. It also regulates the use of CE marking and creates a toolbox of measures for use in product legislation. Source: European Commission, Internal Market, Industry, Entrepreneurship and SMEs
Ransomware	Type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid
Software Bill of Materials (SBOM)	Document or description that provides details about the components used to build a software application.
Open source project	A project that anybody is free to use, study, modify, and distribute your project for any purpose.
Open source software (OSS)	Software that is distributed with its source code, making it available to anyone and for any purpose with all its rights. It grants users the rights to use, study, change, modify and distribute. Open-source software may be developed in a collaborative public manner.
Placing on the market	The first making available of the product on the Union market.
Making available on the market	Any supply of a product for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.
Small and medium-sized companies	An enterprise that satisfies the criteria laid down in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.05.2003, p. 36): employs fewer than 250 persons, has an annual turnover not exceeding €50 million, and/or an annual balance sheet total not exceeding €43 million.
Standard	A technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory. There could be international,

	European, harmonized and national standards.
Supply chain	Network between an entity and its suppliers to produce and distribute a specific product or to provide a certain service to the end user.
Supply chain security	Ensuring appropriate measures concerning security-related aspects of the relationship between and entity and its suppliers or service providers. This may entail for an entity to take account of the vulnerabilities specific to each supplier or service providers, the quality of products and cybersecurity practices of their suppliers and service providers, including security development procedures, etc.
Third party conformity assessment	Under the New Legislative Framework, a conformity assessment that requires the intervention of a third party, e.g. an external conformity assessment body (so-called "notified body"). Such a body must be impartial and fully independent from the organisation or the product it assesses.
Users	Companies, public administrations, consumers as well as any other types of entities that deploy and operate products with digital elements, including essential and important entities covered by the revised NIS Directive (such as operators of critical infrastructure).
Vulnerability	Vulnerabilities are weaknesses in the computational logic of a digital system that, once discovered, provide attackers with an opportunity to breach the system. Article 4(8) of the Commission's proposal for a revision of the NIS Directive (COM(2020) 823 final) defines a vulnerability as a *"weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber threat"*.
Zero-day vulnerabilities	Vulnerabilities discovered by attackers before hardware or software manufacturers become aware of them. As a result, zero-day vulnerabilities can be exploited before the manufacturer has the possibility to develop a fix.

LIST OF TABLES