Council of the European Union

Brussels, 16 September 2022
(OR. en)

12429/22
ADD 3

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 2
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Annexes to the 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 2.

Encl.: SWD(2022) 282 final - Part 2

EUROPEAN
COMMISSION

Brussels, 15.9.2022
SWD(2022) 282 final

PART 2/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Annexes to the 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}

List of Annexes

ANNEX 1: PROCEDURAL INFORMATION

1. Lead DG, Decide Planning/CWP references

Lead DG: Directorate-General for Communications Networks Content and Technology (CNECT).

Decide: PLAN/2022/56.

CWP: Commission Work Programme 2022, Making Europe stronger together (COM(2021) 645 final) under Policy objective A Europe Fit for the Digital Age (initiative number 6).

2. Organisation and timing

The initiative constitutes a core part of the single market and was announced by President von der Leyen in her 2021 State of the Union address. The Commission Work Programme for 2022 envisages the adoption of this Act for Q3 2022 under Policy objective A Europe Fit for the Digital Age (initiative number 6).

It is based on Article 114 TFEU since it aims to improve the functioning of the internal market by setting harmonized cybersecurity rules on all products with digital elements placed on the Union market.

The impact assessment process started with opening of a public consultation and publishing the Call for Evidence for stakeholder comments for a period of 10 weeks from 16 March 2022 until 25 May 2022. For details on the consultation process, see *Annex 2*.

The inter-service group (ISG) met on 28 February 2022 and on 2 June 2022 before submission of the Staff Working Document to the Regulatory Scrutiny Board on 13 June 2022. The ISG consists of representatives of the Secretariat-General, and the Directorates-General CNECT, COMP, JUST, GROW, LS, HOME, SANTE, FISMA, AGRI, JRC, DEFIS, TRADE, ENV, ENER, EMPL, EAC, MOVE, RTD, TAXUD, MARE, EEAS, ECFIN and CLIMA.

3. Consultation of the RSB

On 13 June 2022, the DG CNECT submitted the draft Impact Assessment to the Regulatory Scrutiny Board, in view of a hearing on 6 July 2022.

The Regulatory Scrutiny Board issued a positive opinion with reservations on 8 July 2022.

4. Evidence, sources and quality

The Commission carried out an extensive consultation in preparation of this Impact Assessment report. It benefited from consultation activities already carried out in 2021 for the exploratory study contracted by the Commission and implemented by a consortium made of Wavestone, CEPS, ICF and CARSA to assess the need for horizontal cybersecurity requirements for products with digital elements. To ensure a high level of coherence and comparability of analysis for all potential policy approaches, a second study led by the same consortium was contracted to collect evidence and conduct analyses in the first half of 2022.

In addition to the Commission open public consultation and feedback on the Call for Evidence, the external contractors collected evidence from a variety of stakeholders through targeted interviews with experts covering different domains, focus groups, two

workshops and a targeted online consultation. Moreover, to further support evidence based analysis, the Commission has conducted extensive desk research, covering a wide spectrum of policy studies and reports. They have been quoted in the main body of the Impact Assessment.

The quality of the analytical methods is detailed in Section 6 of this report and *Annex 4* below.

ANNEX 2: STAKEHOLDER CONSULTATION (synopsis report)

1. Consultation scope and objectives

The consultation activities aim at collecting the views of Member State competent authorities, Union bodies dealing with cybersecurity, hardware and software manufacturers, importers and distributors of hardware and software, trade associations, researchers and academia, notified bodies and accreditation bodies, cybersecurity industry professionals, consumer organisations and other users of products with digital elements, and citizens. All these different stakeholder groups are expected to have important information and insights as regards possible actions to improve the cybersecurity of products with digital elements, as well as interest in and opinions on shaping the debate about the possible options for the future.

The stakeholder consultation had two objectives:

(1) collect views on the state of cybersecurity as regards products with digital elements,
(2) and collect views on policy options for a future market intervention and their respective impacts.

It will pose general questions designed to collect feedback from the general public and more technical questions targeting expert stakeholders.

The Commission issued the terms of reference for a second study to assist the Commission in evaluating the existing legal and policy framework and to identify policy objectives and propose and assess the expected impacts of a limited number of policy interventions. The second study run for 10 months from February 2022 until December 2022.

Relevant links:

- Study on the need of cybersecurity requirements for ICT products (link)
- Commission Work Programme 2022 (link)
- Call for Evidence for an impact assessment (link)

2. Mapping of stakeholders

The Commission consulted a broad range of stakeholders listed below according to their interest and presumed expertise in the subject matter:

1. **Member State competent authorities** and bodies (such as national cybersecurity authorities).

2. **Union bodies dealing with cybersecurity** such as the EU's cybersecurity agency ENISA (European Union Agency for Cybersecurity) or CERT-EU (Computer Emergency Response Team for the EU Institutions, bodies and agencies).

3. **Hardware and software manufacturers**, including manufacturers of hardware components, ICSs, computers, mobile phones, Internet-of-Things devices, home automation systems, and non-embedded software, such as operating systems or user applications.

4. **Importers and distributors of hardware and software**, which either import products with digital elements from third countries or distribute them throughout the internal market (such as high street retailers and online shops).

5. **Trade associations** representing hardware and software manufacturers but also importers and distributors, such as DIGITALEUROPE, the European DIGITAL SME Alliance, Orgalim, the Information Technology Industry Council (ITI) or the Interactive Software Federation of Europe (ISFE).

6. **Consumer organisations and users of products with digital elements and citizens**, such as the European Consumer Organisation (BEUC), the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) and companies, in particular operators of essential services and digital service providers under the NIS Directive in their role as users of products with digital elements.

7. **Researchers and academia** (focussing on those with expertise in secure products with digital elements development life cycles and the design of secure products with digital elements).

8. **Notified bodies and accreditation bodies**, which play an important role in implementing EU product regulations that are based on the NLF.

9. **Cybersecurity industry professionals**, such as pen testers and white hat hackers.

3. Consultation activities

The consultation activities aimed to obtain input on the five main evaluation criteria based on the EU Better Regulation Guidelines (effectiveness, efficiency, relevance, coherence, EU-added value) as well as the potential impacts of possible options for the future. Both the open public consultation and the targeted surveys developed by the study contractor were structured according to the logic of the five criteria.

The following consultation activities were organised:

- ✓ **A first study:** In December 2021, the Commission has published a study on the need of cybersecurity requirements for products with digital elements[1], which had been conducted by a consortium consisting of ICF, Wavestone, CARSA and CEPS (the exploratory study). The exploratory study has identified several market failures leading to a suboptimal level of cybersecurity of products with digital elements. It has further analysed existing EU and national legislation, and assessed possible regulatory interventions. It concludes that a horizontal legislation laying down requiring across sectors would represent the most cost-effective policy option, creating greater security in the Single Market while enhancing business competitiveness. However, it also concluded that the Commission should perform a more comprehensive and quantitative assessment of the potential policy options.

- ✓ **An Open Public Consultation** with questions targeting citizens, stakeholders and cybersecurity experts. It included questions regarding the current state of cybersecurity as regards products with digital elements. It focused on policy options

[1] https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products

for a potential regulatory intervention. The survey contributed to the collection of diverse opinions and experiences from all stakeholder groups. A smaller set of questions was available to all participants. Respondents such as professionals in the field, or organisations with specific knowledge and expertise were directed to respond to a set of targeted questions within the same online survey. The Public Consultation, implemented according to the Commission's Better Regulation Guidelines for stakeholder consultations, was carried out for a 10-week period, starting in March 2022. The questionnaire was made available in all 24 official EU languages, ensuring that the public consultation is accessible to as many stakeholders as possible, especially citizens.

- ✓ **Surveys** organised by the contractor. An online survey was launched on 16 May 2022 and gathered 24 responses at the time of the finalisation of the impact assessment. The participants were handpicked to cybersecurity experts with an understanding in the areas of cybersecurity public policy, cybersecurity requirements and potential compliance and enforcement costs. The survey was designed to receive detailed feedback on the various aspects of the different policy options, as opposed to the public consultation, the purpose of which was to receive general high-level feedback by a wide range of stakeholders, including non-experts. Participants were presented with the different policy options, and the detailed requirements under policy option 4. Participants were requested to provide cost estimations on compliance and enforcement costs and to provide feedback on the other types of impacts.

- ✓ **Workshops organised by the contractor.** Two workshops have been organised, gathering around 100 representatives from all 27 Member States representing competent authorities, hardware and software manufacturers, importers, distributors, notified bodies, accreditation bodies, and cybersecurity experts. The workshops took place in April and May 2022 and were in addition to the three workshops organised in the framework of the exploratory study.

  - ✓ *Workshop #1* on scope and definitions, policy interplay and cybersecurity requirements. The workshop took place online on 28 April 2022. The study supporting the Commission preparatory work for the upcoming regulatory intervention was presented. In three interactive sessions the scope and definition, policy interplay and cybersecurity requirements were discussed with the stakeholders. 115 people participated, representing industry, governmental agencies, consumer organisations and universities.

  - ✓ *Workshop #2* on risk profiles, conformity assessment procedures and likely impacts. The workshop took place online on 10 May 2022. There were 108 participants. Around half of which represented industry (interests) and around one third represented participants from the public sector across various member states. Other participants included EU agencies, universities and consumer organisations.

    For the respondents, the main driver for a risk categorization (potential physical harm, use, and potential misuse) was dependent on the specific example provided. Most respondents indicated that conformity assessments other than self-assessment could be necessary (84 %). Expected costs as consequences of requirements ranged from “low” for internal product testing/self-assessment, to

"high" for security updates and whole life cycle requirements. For all other requirements, "medium" received the most votes.

- ✓ **Expert interviews** were conducted to gain a deeper understanding of current cybersecurity challenges related to products with digital elements, and to discuss policy options for a potential regulatory intervention. The experts were selected by the Commission who also conducted the interviews during the first and second quarters of 2022. Experts included engineers developing digital hardware and software products, professional users, and representative of consumer organisations. This added to the 52 "semi-structured interviews" that were carried out by the exploratory study.

- ✓ **Bilateral discussions with national cybersecurity authorities, the private sector and consumer organisations.** The Commission reached out to national cybersecurity authorities and private sector and consumer representatives during the first and second quarters of 2022.

- ✓ **Reports by the Contractor,** as part of the study supporting the Commission preparatory work for the Cyber Resilience Act.

4. SME test - consultations with SMEs

Additional efforts have been made to gather views from SMEs on the impact of the policy options. However, it has been very difficult to get substantial input from SMEs. SMEs have been included in the consultation activities as follows:

- The initiative was discussed at the SME envoy network and classified as "relevant" on 6 April 2022.[2]

- The public consultation, targeted survey on impacts and workshops have been disseminated through the GROW Small Business Act network of EU SME business associations and the European Enterprise Network (cooperation with GROW A.2. unit). Due to time constraints, it was not possible to carry out a proper SME panel consultation (which requires to be open for 8 weeks, language translations needed, EUsurvey required, and a summary of results after the consultation).

- In addition, DG CNECT presented the initiative at several meetings with various SME associations. For instance: GROW Meeting with SME stakeholders on Wednesday 11 May 2022; Joint conference on 10 May 2022 of the European industry federations Europump (European Pumps Industry Association), CEIR (European Taps and Valves Industry Association) and Pneurop (European compressors, vacuum pumps and pneumatic tools industry association; presentation and discussion of the regulatory intervention at the European Digital SME Alliance working group on cybersecurity on 5 May 2022.

- **Targeted outreach** was done to key SME stakeholders, such as the Digital SME Alliance and their individual members. In the context of the study supporting this report, a targeted list of SMEs was established to be invited to the workshops. In

[2] https://ec.europa.eu/docsroom/documents/50041

addition, several interviews were done with SMEs related to the impacts of the initiative.

Outcome of the consultation activities:

- In the context of the public consultation, only few individual companies representing SMEs participated (14 in total). This included 7 medium-sized companies (50 to 249 employees), 5 small-sized companies (10 to 49 employees), and 2 micro-sized companies (1 to 9 employees).

- In order to achieve a more representative panel of responses, trade associations representing SMEs have also been considered. In total, 47 organisations representing SMEs have been identified, including providers, users, trade associations and other types of companies (e.g. service providers).

- A number of SMEs participated in the workshops: out of the 223 participants in the workshops 1 and 2, 19 participants represented SMEs, including individual companies and trade associations.

5. Consultation webpage & communication activities

Anyone interested was able to provide feedback at different stages of the policy cycle on the Have your say page. Stakeholders that wished to be notified by e-mail on new public consultations could follow the RSS Feed or subscribe to Commission at work – Notifications.

6. Synopsis report of the open public consultation

Profile of respondents

A total of **167 responses to the OPC were received**. Almost two-thirds of responses came from companies/businesses and business associations (35.3% and 28.1% respectively), while 13% of responses came from public authorities. 7.8% of responses came from EU citizens, 2.4% of responses each from consumer organisations and non-governmental organisations (NGOs). 1.8% came from academic/research institutions and 1 response from a trade union. In total, 59 companies/businesses responded. Among them, 45 were large, 7 medium, 5 small, and 2 micro.

Turning to responses received by the country, more than half of the responses came from Belgium (44; 26.3%) and Germany (43; 25.7%) while 22 responses came from non-EU countries (13 from the United States). No responses were received from the following Member States: Croatia, Cyprus, Ireland, Latvia, Lithuania, Luxembourg, Malta, Portugal, Romania, Slovakia, and Slovenia.

Q1: Overall level of cybersecurity of products with digital elements

Respondents were asked to **rank the overall level of cybersecurity of products with digital elements marketed within the European Union** on a scale from 1 to 5 with 5 indicating a very high level of cybersecurity. The majority of respondents (53%) indicated that the overall level of cybersecurity is reflected at level 3, while 23% of respondents indicated level 2 and 12% indicated level 4. There were no significant differences between respondent types.

The majority of large companies (55%) ranked the overall level of cybersecurity of products with digital elements marketed within the European Union with a 3. Medium companies were split, although 43% of their responses also indicated level 3. Among the small and micro companies, level 3 was also reflected in the majority of responses – 50% of micro companies and 40% of small companies. For small companies, the rest of the responses were equally split between levels 1, 2 and 5 (20% each).

Respondents were also asked to elaborate on their answers. Most respondents have stated that **an average level of cybersecurity across all types of products with digital elements is difficult to establish as certain differences can be observed** across sectors, product types or whether they are marketed for businesses or consumers. Several respondents have highlighted **different gaps and obstacles hindering progress** that they observed in the overall level of cybersecurity of products with digital elements. Conversely, several respondents have also indicated **signs of progress and improvements** they observed.

Q2: Level of risk of cybersecurity incidents

Respondents were asked **how the level of risk of cybersecurity incidents affecting products with digital elements has evolved during the last five years**. The majority of respondents (54%) indicated that the risk level has increased significantly and 40% of respondents indicated that the risk level has increased. Only a small minority of respondents (4%) indicated that the risk level has remained the same over the last 5 years and only 1% of respondents mentioned the risk level has decreased significantly. There were no significant differences between respondent types.

The majority of large companies have indicated that the risk level has increased – 38% of them have indicated that the risk level has increased and a further 49% indicated that the risk level has increased significantly. The majority of medium companies (57%) also indicated that the risk level has increased significantly and all (100%) micro companies indicated the same response. Among small companies, the majority of responses indicated that the risk level has increased: 40% indicated the level has increased, and a further 40% indicated that it increased significantly.

Respondents were also asked to elaborate on their answers and they provided various types of **examples of cybersecurity threats that have been observed to increase during recent years**. Several respondents also indicated **underlying causes (e.g. the proliferation of interconnected devices on the market, increased reliance on technology due to remote working, increased sophistication of attacks, geopolitical tensions)** that they think are increasing the risk level of cybersecurity threats. Other respondents have indicated that **the real level of risk is sometimes difficult to assess**.

Q3: Impact of cybersecurity incidents affecting products with digital elements

Respondents were asked to score several **possible consequences of cybersecurity incidents based on their actual negative impact on them or their organisation** by using a scale from 1 to 5 with 5 indicating a very high negative impact. The consequences that have been ranked the highest in terms of their negative impact were ‘reputational damage’ and ‘financial cost of disruption’ (e.g. due to a ransomware attack), as they have both been ranked with an average of 4. However, very close to this level of perceived negative impact were also ‘damage to fundamental rights’ (3.8 average score), ‘financial cost of implementing measures to respond to a cybersecurity incident’

(3.8 average score) and 'compromising the security of our economy and society' (3.7 average score). There were no significant differences between respondent types.

Company size breakdown:

5. **The financial cost of implementing measures to respond to a cybersecurity incident:** The majority of large companies (47%) and the majority of medium companies (57%) selected level 4. Micro companies' responses were equally split (50%) between levels 4 and 5, while small companies were also equally split on levels 4 and 5 (40% each), with the rest of 20% of votes being cast to level 3.
6. **The financial cost of disruption (e.g. due to a ransomware attack):** Large companies indicated mixed responses: 31% for level 5, 20% for level 5 and 15% each for levels 2 and 3. The majority of medium companies (43%) indicated level 4, while 40% of small companies indicated and a further 40% of them indicated level 5. Micro companies were equally split (50%) between levels 4 and 5.
7. **Reputational damage:** Most responses from large companies were equally split between levels 3, 4 and 5 (24% each), while only 7% of responses went to each levels 1 and 2. The majority of medium companies (43%) indicated level 4, the majority of small companies were split between levels 4 and 5 (40% each) and micro companies were equally split between levels 4 and 5 as well (50% each).
8. **Compromising the security of our economy and society:** 27% of responses from large companies indicated level 4, 18% the levels 3 and 5 each and only 16% indicated level 2. The majority of medium companies (43%) and all (100%) micro companies indicated level 5 while small companies were equally split between levels 1 to 5 (20% each).
9. **Damage to health and life:** The majority of large companies indicated levels 1 (24%) and 2 (27%). Only 9% indicated levels 5, and 11% indicated each level 3 and 4. Among the medium companies, most responses were received by level 5 (29%). However, 28% of medium companies also refrained from responding here. The majority of small companies (60%) indicated level 2. The rest of the responses were split between levels 1 and 4 (20% each). Micro companies were equally split between levels 3 and 5 (50% each).
10. **Damage to fundamental rights (e.g. privacy, protection of personal data, consumer protection):** Responses from large companies were mixed: most responses from large companies indicated level 4 (22%) and 20% each were allocated to levels 2 and 4, while 16% indicated level 3. The majority of medium companies (43%) indicated level 5, while the majority of small companies (40%) indicated level 3. The remaining responses by small companies were equally split between levels 2, 4 and 5 (20% each). Micro companies were equally split between levels 4 and 5 (50% each).
11. **Environmental damage:** The majority of responses from large companies were split between level 1 (23%) and level 2 (31%). The majority of responses from medium companies were similarly split between levels 1 (28%) and 2 (22%), with a further 14% allocated to level 3. For medium companies, levels 1 and 3 received 19% of responses each. 46% of medium companies refrained from answering this question. Within small companies, 32% indicated level 2 and a further 24% indicated level 1. 40 micro companies did not indicate a level, and among those which did, the most responses went to levels 1 and 4 (16% each).

Respondents were also asked to elaborate their answers. Several stakeholders have indicated that for certain sectors (e.g. healthcare) or certain types of companies (e.g. SMEs) the negative impacts of cybersecurity incidents are more prominent. Other

stakeholders have also reiterated the link between the consequences of cybersecurity incidents to their underlying causes or to the circumstances in which they appear. Several stakeholders have also pointed out that certain negative consequences are already covered by existing sectoral legislation.

Q4: Impact on users

Respondents were asked to rank several **impacts on users based on their agreement with the statement** on a scale from 1 to 5 with 5 indicating that they fully agree with it. As a result, respondents indicated that they mostly agree with the fact that the user bears additional costs due to the need to deploy highly-priced technical security solutions (ranked with an average of 4) and with the fact that the user bears the additional cost when affected by a cybersecurity incident (also ranked with an average 4). The statement 'the user bears additional costs due to highly-priced cybersecurity insurance was ranked slightly lower at 3. There were no significant differences between respondent types. There were no significant differences between respondent types.

Company size breakdown:

- **The user bears the additional cost when affected by a cybersecurity incident:** Most large companies were split between levels 4 (38%) and 5 (33%). Most medium companies were also split between levels 4 (29%) and 5 (29%). The majority of small companies (40%) and all micro companies (100%) indicated level 5.
- **The user bears additional costs due to highly-priced cybersecurity insurance:** Responses from large companies were mixed: 22% indicated level 4, 16% indicated level 5, while 20% indicated level 2 and a further 11% level 3. Among medium companies, most respondents indicated level 3 while levels 2, 4 and 5 received each 14% of responses. The majority of small companies (40%) indicated level 2, while micro companies were equally split (50%) between levels 4 and 5.
- **The user bears additional costs due to the need to deploy highly-priced technical security solutions:** Most responses from large companies were split between levels 3 (22%), 4 (26%) and 5 (27%). Similarly, among medium companies, most responses were split between levels 3 (14%), 4 (29%) and 5 (29%). The highest number of small companies (40%) indicated level 3 while micro companies were equally split (50%) between levels 2 and 5.

Respondents were also asked to elaborate their answers. Several stakeholders detailed their responses by indicating **how the impacts on users differ based on certain specific circumstances** (e.g. whether the user is a consumer or a professional user, the size of the user, type of products with digital elements in case, whether the market is B2B or B2C). Several stakeholders also had **specific comments regarding the cyber insurance market, especially concerning the increased cost of insurance premiums**. Other stakeholders have indicated **additional impacts** (such as the psychological impact or loss of confidence in products with digital elements) that they think will affect the users.

Q5: Awareness and understanding of cybersecurity properties of products with digital elements

Respondents were asked the extent to which they were **aware of the cybersecurity risks associated with products with digital elements** (on a scale from 1 to 5 with 5 indicating

that they strongly agreed)**:** 79% declared to be either aware or strongly aware; only 4% were not aware of security risks linked to products with digital elements.

Company breakdown: 75% of large companies agreed with this statement; 48% of medium companies agreed, while 24% were neutral; most (67%) small companies also agreed; micro companies generally agreed (55%); were neutral (10%) and disagreed (25%).

The survey asked whether there is **sufficient and clear information about the cyber security properties of products with digital elements** (on a scale from 1 to 5 with 5 indicating that you strongly agreed)**:** 46% of respondents believed that this was not the case; 33% of them had neutral feelings, while only 17% thought there was enough information.

Large companies generally disagreed (38%) or were neutral (38%); medium companies also disagreed (56%) or were neutral 29%; small companies disagreed (42%) or were neutral (33%); micro companies disagreed (35%) or were neutral (40%).

Respondents were asked about the extent to which **they understood the cybersecurity properties of products and had the skills to operate them securely** (on a scale from 1 to 5 with 5 indicating that they strongly agreed): 64% of them agreed or strongly agreed with this statement; 16% were neutral, and 14% did not believe to understand cyber security properties or have the competencies to use products securely. It has to be specified in this context that even if the percentage of respondents agreeing with this statement is high, it should be interpreted in view of the categories of respondents that were predominantly replying to the public consultation (namely cybersecurity experts) and that only very few citizens participated in the survey.

75% of large companies agreed; medium companies generally agreed (57%) and 24% disagreed; small companies generally agreed (54%), but 29% disagreed.

The survey asked whether respondents **valued products' usability and price over cyber security features** (on a scale from 1 to 5 with 5 indicating that they strongly agreed): 46% of them disagreed with this statement; 33% neither disagreed nor agreed and only 12% seemed to privilege usability and price over cyber security.

Most large companies disagreed (52%) or were neutral (31%); 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%).

Q6: The role of the manufacturers in addressing cybersecurity vulnerabilities and incidents

Respondents were asked whether **hardware manufacturers were effectively addressing the cybersecurity vulnerabilities and incidents affecting their customers** (on a scale from 1 to 5, with 5 indicating that they strongly agreed): 37% thought this was not the case; 29% were neutral; 28% thought they were being effective.

Company breakdown: large companies mostly disagreed (35%), were neutral (32%) and agreed (29%); medium companies mostly disagreed (50%) or were neutral (27%); small companies mostly disagreed (50%) or were neutral (20%); micro companies generally agreed (50%) or were neutral (25%).

The survey asked the extent to which **software manufacturers were effectively addressing the cybersecurity vulnerabilities and incidents affecting their customers**

(on a scale from 1 to 5, with 5 indicating that they strongly agreed): 33% disagreed or strongly disagreed software manufacturers were effectively doing it; 30% were neutral, and 34% believed they were instead effective.

Large companies disagreed (35%) or agreed (35%); medium companies disagreed (32%), were neutral (27%) or disagreed (27%); small companies disagreed (37%) or were neutral (33%) and only some agreed (21%); micro companies mostly agreed (45%) or were neutral (25%).

Q7: Aspects having the biggest impact on manufacturers' decisions related to cybersecurity of products with digital elements

Most manufacturers (65%) reported that **the potential reputational damage and the loss of users' trust following an incident** were very relevant factors in their decision-making regarding the cyber security of their products with digital elements.

74% of large companies thought it was very relevant, compared to 36% of medium enterprises; 47% of small companies believed it was relevant too, compared to 93% of micro companies.

Most manufacturers (77%) declared that **customer expectations, including contractual obligations**, were either relevant or very relevant in their decision-making regarding the cybersecurity of their products with digital elements; 20% did not have an opinion about it.

Companies opted for either relevant or very relevant: large (84%); medium (64%); small (65%) or micro (93%).

Most manufacturers (66%) agreed or strongly agreed that **public procurement practices** had a big impact on their decision making regarding the cybersecurity of their products with digital elements; 24% did not know.

Companies opted for either relevant or very relevant: large (72%), medium (36%), small (58%) and micro (86%).

Respondents also pointed out **other aspects which influence their decision-making regarding the cyber security of products with digital elements**, including (ranked based on frequency, from most to least mentioned): threat scenario (i.e. cyber security risks and attack vectors); type and intended use of the product; general security standards and requirements, deriving from compliance, legislation and best practices; safety concerns; other requirements, such as usability and interoperability; supply chain; production, operation, and maintenance costs.

Q8: Cybersecurity of products with digital elements in the product life cycle

Respondents were asked **the extent to which hardware and software manufacturers took the cybersecurity of their products with digital elements into account in the design phase** (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously) of a product life cycle and the results ranged mainly from not seriously (29%), neutral (19%) and seriously (21%).

Large companies thought it was taken seriously (40%) but also not seriously (33%); most medium companies (52%) believed it was not taken seriously; most small companies were neutral (27%) or thought it was not taken seriously (36%); 48% of micro companies believed it was taken seriously.

Respondents were asked **the extent to which hardware and software manufacturers took the cybersecurity of their products with digital elements into account in the development phase** (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously) of a product life cycle and the results ranged mainly from not seriously (25%), neutral (26%) and seriously (19%); an additional 16% thought that these are taken very seriously.

Large companies generally indicated it was taken seriously (42%) or not taken seriously (32%); medium companies thought it was not taken seriously (47%) or were neutral (19%); small companies believed it was taken seriously (33%) and not seriously (29%).

Respondents were asked about **the extent to which hardware and software manufacturers took the cybersecurity of their products with digital elements into account during the release of the product on the market phase** (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously) of a product life cycle and results ranged mainly from not seriously (25%), neutral (26%) and seriously (21%).

34% of large companies thought it was taken seriously and 29% were neutral; 47% of medium companies believed it was not taken seriously; 36% of medium companies were neutral and 27% thought it was not taken seriously; 47% of micro companies believed it was taken seriously and 14 were neutral.

Respondents were asked **the extent to which hardware and software manufacturers took the cybersecurity of their products with digital elements into account after the release of a product, namely maintenance and evolution of the product phase** (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously), and results ranged mainly from not seriously (24%), neutral (32%) and seriously/very seriously (27%).

Companies of all sizes were generally neutral or tended to think it was not taken seriously: large (37%); medium (47%), and small (27%). Only micro companies thought it was taken seriously (33%) compared to non-seriously (14%).

Q9: Effectiveness of measures to increase cyber security of products with digital elements

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure would be very effective) **guidelines or recommendations for the development of secure products with digital elements issued at the EU level addressed to manufacturers** could be effective in increasing the cybersecurity of products with digital elements marketed in the EU: almost half (47%) agreed these could be effective, while 27% were neutral; 25% did not believe these measures would be effective.

Companies of all sizes tended to think these could be effective: large (49%); medium (29%), small (45%) and micro (59%) or were generally neutral (respectively, 20%, 38%, 46% and 23%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure would be very effective) **further voluntary European cybersecurity certification schemes** for products with digital elements and services could be effective in increasing the cybersecurity of products with digital elements marketed in the EU: 37% disagreed these could be effective; 31% were neutral, and 31% agreed these measures would be effective.

40% of large and 46% of medium companies stated they could be effective; 33% of small companies thought they could be effective and the same percentage believed the opposite; micro companies were mainly neutral (36%) or thought they could be effective.

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure would be very effective) **EU public procurement guidelines** taking into account cybersecurity requirements could be effective in increasing the cybersecurity of products with digital elements marketed in the EU: 60% agreed these could be effective; 28% were neutral; 9% disagreed these measures would be effective.

Most companies gave neutral answers or tended to agree these could be effective: large (56%); medium (63%), small (58%) and micro (55%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure would be very effective) **amending existing legislation regulating specific products with a digital dimension** (such as the legislation on lifts or gas appliances) could be effective in increasing the cybersecurity of products with digital elements marketed in the EU: 51% agreed these could be effective; 17% were neutral; 27% disagreed these measures would be effective.

55% of large companies believed it could be effective and so did 54% of medium ones; small companies had mixed feelings but 46% also believed they could be effective; 36% of micro companies instead declared these might not be effective or were neutral about it (31%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure would be very effective) **introducing mandatory horizontal cybersecurity requirements for hardware products** could be effective in increasing the cybersecurity of products with digital elements marketed in the EU: 72% agreed these could be effective; 13% were neutral; 10% disagreed these measures would be effective.

Most companies of all sizes thought these could be effective, namely large (73%), medium (71%), small (67%) and micro (81%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure would be very effective) **introducing mandatory horizontal cybersecurity requirements for software products** could be effective in increasing the cybersecurity of products with digital elements marketed in the EU: similarly to the question above, 74% agreed these could be effective; 10% were neutral; 11% disagreed these measures would be effective.

Most companies of all sizes believed these could be effective, namely large (76%), medium (71%), small (81%) and micro (66%).

When asked to elaborate on their answers, respondents highlighted the following themes: Mandatory **horizontal legislation is the preferred option** vs "softer" approaches (as already found in the survey above); Requirements must be **clear as well as limit fragmentation/duplication**; Alignments with **existing legal instruments**.

Q10: Requiring manufacturers to act

Respondents were asked to assess the impact (on a scale from 1 to 5 with 5 indicating that a measure would have a very high impact) of **requiring manufacturers to make available information and provide instructions on securely installing, operating and using the product** in question: 70% reported this would have a high or very high impact; 22% were neutral, and 8% suggested this would have a low or very low impact.

Most companies of all sizes thought this could have a high impact, namely large (71%), medium (67%), small (54%) and micro (90%).

Respondents were asked to assess the impact (on a scale from 1 to 5 with 5 indicating that a measure would have a very high impact) of **requiring manufacturers to take corrective actions** (such as patching, recalling or withdrawing a product) when a product is found to be not secure: 86% reported this would have a high or very high impact; 7% were neutral and 7% suggested this would have a low or very low impact.

Most companies of all sizes thought this could have a high impact, namely large (83%), medium (88%), small (83%) and micro (95%).

Q11: Relevance of cyber security measures to users

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure is very relevant) making available **technical documentation** (containing information to demonstrate the conformity of the product to the applicable requirements) on the cybersecurity properties of a product (such as on risks and proper use) would help users assess cybersecurity properties of products with digital elements: 47% reported this would be relevant or very relevant; 26% were neutral and 25% suggested this would not be relevant.

Companies of all sizes generally thought this could be relevant, namely large (49%), medium (46%), and micro (55%); small companies were mostly neutral (39%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure is very relevant) making available an **EU Declaration of conformity** (stating that all the relevant requirements of the applicable legislation are satisfied) would help users assess cybersecurity properties of products with digital elements: 51% reported this would be relevant or very relevant; 25% were neutral and 19% suggested this would not be relevant.

Companies were either neutral or tended to agree this could be relevant, namely large (57%), medium (33%), small (46%) and micro (41%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure is very relevant) **affixing a symbol of compliance** such as CE marking would help users assess the cybersecurity properties of products with digital elements: 51% reported this would be relevant or very relevant; 22% were neutral and 22% suggested this would not be relevant.

Most large (57%), small (50%) and micro (41%) companies stated this could be relevant; medium ones instead either disagreed (38%) or were neutral (29%).

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that a measure is very relevant) **training on the secure use of products with digital elements** would help users assess the cybersecurity properties of products with digital elements: 57% reported this would be relevant or very relevant; 23% were neutral and 17% suggested this would not be relevant.

Most companies of all sizes declared this could be effective, namely large (50%), medium (54%), small (63%) and micro (73%).

Respondents elaborated upon their answers and highlighted the following themes: Equipping users with the right cyber security knowledge; Security information provided to users should be easy and understandable; Be clear about the expected lifetime of a

product and consequential security updates; A symbol/label of compliance could also be useful.

Q12: Effectiveness of cyber security requirements subjecting different products and services

Respondents were asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed) they believed **subjecting hardware products** marketed in the EU to cybersecurity requirements would be an effective measure: 67% either agreed or strongly agreed; 16% were neutral and 10% either disagreed or strongly disagreed.

Most companies of all sizes declared this could be effective, namely large (65%), medium (58%), small (60%) and micro (56%).

Respondents were asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed) they believed **subjecting embedded software** marketed in the EU to cybersecurity requirements would be an effective measure: 77% either agreed or strongly agreed; 9% were neutral and 9% either disagreed or strongly disagreed.

Most companies of all sizes declared this could be effective, namely large (77%), medium (83%), small (79%) and micro (59%).

Most companies of all sizes declared this could be effective, namely large (57%), medium (54%), small (63%) and micro (59%).

Respondents were asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed) they believed **subjecting hardware products with higher cybersecurity risks** marketed in the EU to cybersecurity requirements would be an effective measure: 85% either agreed or strongly agreed; 4% were neutral and 4% either disagreed or strongly disagreed.

Most companies of all sizes declared this could be effective, namely large (82%), medium (88%), small (83%) and micro (86%).

Respondents were asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed) they believed **subjecting all standalone software products** marketed in the EU to cybersecurity requirements would be an effective measure: 58% either agreed or strongly agreed; 19% were neutral and 16% either disagreed or strongly disagreed.

Most companies of all sizes declared this could be effective, namely large (59%), medium (54%), small (63%) and micro (56%).

Respondents were asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed) they believed **subjecting software products subject to higher cybersecurity risk** marketed in the EU to cybersecurity requirements would be an effective measure: 86% either agreed or strongly agreed; 18% were neutral and 5% either disagreed or strongly disagreed.

Most companies of all sizes declared this could be effective, namely large (84%), medium (92%), small (83%) and micro (82%).

Respondents elaborated upon their answers and highlighted the following topics: Any EU legislation should adopt a **risk-based approach**; The importance of **clear definitions and scope**.

Q13: Appropriateness of existing EU regulation

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed with a statement) existing EU regulations appropriately addressed cybersecurity of **tangible products with digital elements** (hardware) throughout their life cycle: 41% of respondents either strongly disagreed or disagreed; 28% were neutral and 13% either agreed or strongly agreed.

Large companies selected 3 (33%) and 2 (24%). Medium companies opted for 2 (67%). Small companies were divided into 1, 2, 3 and 5 (20% for each). Micro companies were evenly split between 3 and 4.

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed with a statement) existing EU regulation appropriately addressed cybersecurity of **intangible products with digital elements (software)** throughout their life cycle: 46% of respondents either strongly disagreed or disagreed; 28% were neutral and 12% either agreed or strongly agreed.

Large companies opted for 2 (33%) and 3 (31%). Medium companies chose 2 (50%), while small companies 1 (40%). Micro companies were evenly split between 3 and 5.

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating that they strongly agreed with a statement) existing EU regulation appropriately addressed **all relevant cybersecurity risks (material and non-material damages) related to the use or misuse of a product with digital elements**: 43% of respondents either strongly disagreed or disagreed; 25% were neutral, and 15% either agreed or strongly agreed.

Large companies chose 3 (32%) and 2 (22%), while 50% of Medium companies opted for 2. Small companies were divided for all responses (20% each), except for 2. Micro companies were equally divided between 2 and 5.

Q14: Risk of increasing costs and legal uncertainty in the absence of an EU initiative

The survey asked the extent to which (on a scale from 1 to 5 with 5 indicating they fully agreed) there was a **risk of increasing costs and legal uncertainty for market stakeholders in the absence of an EU initiative**, namely in a scenario in which the Member States could adopt national laws placing certain requirements on manufacturers as opposed to horizontal cybersecurity requirements at European level: 85% either agreed or strongly agreed; 9% were neutral and 4% either disagreed or strongly disagreed.

Most companies of all sizes declared this could be effective, namely large (86%), medium (83%), small (92%) and micro (86%).

Respondents elaborated upon their answers and almost unanimously concluded that an **EU-wide initiative was to be preferred** compared to single initiatives at the member state level.

Q15: Legal requirements related to the cybersecurity of products with digital elements for manufacturers

Respondents who identify as manufacturers were asked to respond whether their products with digital elements are subject to **legal requirements as regards their cybersecurity**. They were also advised to take into account in their answer European, national but also legislation stemming from third countries. The majority of respondents who replied to this question (65%) indicated that their products with digital elements are subject to legal requirements as regards their cybersecurity, while only 3% indicated the opposite. Out of

the 65% of respondents who indicated 'yes', the vast majority were represented by business associations (25% of responses) and companies/business organisations (37% of responses).

The majority of large companies (67%) indicated that their products with digital elements are subject to legal requirements as regards their cybersecurity. 28% of medium companies also responded positively although 43% indicated that they are not concerned by this question and a further 29% did not respond. The majority of small companies (60%) and 50% of micro companies also responded although the other 50% of micro companies did not provide an answer.

Respondents were also asked to indicate **which of their products with digital elements are subject to which legal requirements as regards their cybersecurity and to specify the relevant product categories and applicable legislation**. The following categories of products were mentioned together with the applicable legislation: information and communications technology (ICT) products, services, and processes – are subject to certification frameworks under the Cybersecurity Act (EU/2019/881); radio equipment (electrical and electronic equipment that can use the radio spectrum for communication and/or radio determination) - is subject to Radio Equipment Directive. The proposed delegated act (2021) expands that scope from smart appliances and cameras to connected radio equipment like cell phones, laptops, alarm systems, wearable health monitoring devices, home automation, and other internet-connected devices; digital services providers (online search engines, online marketplaces, and cloud computing services) – are subject to the security of the Network and Information Systems Directive (NIS 2.0); motor vehicles – are subject to Regulation 2018/858 on type approval for motor vehicles; Regulation (EU) 2019/2144 (General Safety Regulation), and UN Regulation 155 on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system; UN Regulation 156 on software updates and software management system; Regulation 2014/53 Radio Equipment Directive (for radio equipment of motor vehicles); medical products – subject to Medical Device Regulation, In-Vitro Diagnostic Regulation, Machinery Directive, General Product Safety Directive, Radio-Equipment Directive (RED-DR not for MDR/IVDR products but in scope for accessories and non-medical products); financial products – subject to PSD2, EBA-Guidelines, requirements of the European Central Bank, NIS-Directive, future Digital Operational Resilience Act (DORA), BSI Act (BSIG), Prudential requirements for IT (BAIT).

Other types of horizontal legislation (from the EU and third countries) mentioned by several stakeholders were: the EU's General Data Protection Regulation – which covers the requirements related to protecting data, and breach reporting; the California Consumer Privacy Act and California IoT Cybersecurity Law; products in the scope of the Sales of Goods Directive (EU) 2019/771 need to provide security updates; the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Q16: Responsibility of hardware and software manufacturers

Respondents were asked whether **hardware and software manufacturers should be responsible for the full life cycle of a product with digital elements** (such as by being required to provide updates). The vast majority of respondents (88%) indicated a positive

answer to the question, while only 9% indicated a negative one. There were no significant differences between respondent types.

Responses were in their majority affirmative for all sizes of companies: 80% of large companies, 86% of medium companies and 100% of both small and micro companies.

Respondents who indicated that hardware and software manufacturers should be required to provide security updates were also asked for **how many years should they be required to do so**. Most respondents (13%) who provided several fixed numbers of years for this obligation indicated 5 years as the ideal period for which hardware and software manufacturers should be required to provide security updates. 9% of respondents also indicated 10 years as their ideal timeframe, while only 7% of respondents indicated a lower timeframe of 3 years.

Most large companies refrained from responding (40%) or preferred to provide other responses than the ones indicated (40%). Likewise, 60% of small companies preferred to offer another response. The same applies to medium companies as 43% did not respond and 29% did not know or had no opinion. However, 14% each indicated 3 and 4 years as their responses. Micro companies' responses were equally split between 1 and 10 years.

The majority of stakeholders (51%) who responded to this question chose to detail their response rather than pick a fixed number of years. Several responses indicated that the **obligation should exist for the entire life cycle** of the hardware/software product. A few responses also **disagreed** with the idea of an obligation that would exist throughout the entire life cycle of the hardware/software product. Others stressed that **the timeframe of the obligation should be adapted** based on the type of hardware/software product provided or other specific circumstances. Others stressed that **providing updates is not sufficient**.

Q17: Approaches contributing to the cybersecurity of a product with digital elements

Respondents were asked to rank **to what extent several approaches contribute to the cybersecurity of a product with digital elements** by using a scale from 1 to 5 with 5 indicating that the measure would be very effective. The measure deemed most effective and which received the higher score (4.8) was the measure indicating that 'cybersecurity is taken into account during all phases of the development process (security by design)'. The next best average score was 4.7 and was awarded by respondents to the measure stipulating that 'Hardware and software manufacturers provide updates when vulnerabilities are discovered, including after a product has been put on the market'. At the other end of the spectrum, the measure deemed least effective and which received the lowest score (3.3) stipulated that 'Hardware and software manufacturers should make available to relevant stakeholders (e.g. end-users) a list containing the details and supply chain relationships of various components used in building the product with digital elements (so-called Software Bill of Materials)'. There were no significant differences between respondent types.

Respondents were also asked to indicate which **other measures taken by hardware and software** manufacturers **could improve the cybersecurity of products with digital elements**. Among the additional measures that have been indicated were: the utilisation of strong technical protection mechanisms, including encryption; an improved mechanism for assistance from national security/cybersecurity authorities to help the private sector address dynamic cybersecurity risks; continuous education, training and assessment of the personnel of the organization to the specific requirements, implementation mechanisms, secure coding principles, etc.; manufacturers must be

required to effectively communicate the supply chain relationship of the myriad of components, from different hardware and software manufacturers , that make up the IoT device; manufacturers should assure the robustness of their software/service towards ransomware attacks. For instance, measures that protect already stored backups from being modified, requiring multi-factor authentication for access to backup infrastructures, requiring separate authentication for application management and backup infrastructure management, penetration testing backup infrastructure annually, testing reinstallation of backups periodically etc.; training of consumers, especially vulnerable consumers; the adoption of bug bounty programs; open-source approach/sources open and auditable; commitment to the Digital Responsibility Goals; for the critical software/hardware products, periodic recertification/testing of software and hardware products by independent 3rd parties and government entities.

Q18: Approaches regarding higher risk products with digital elements

Respondents were asked **whether products with digital elements with a higher risk should be subject to a stricter process of demonstrating conformity with cybersecurity requirements**. The vast majority of respondents (88%) indicated an affirmative answer while only a small minority (5%) disagreed. There were no significant differences between respondent types.

Companies of all sizes also overwhelmingly responded yes: large (84%), medium (83%), small (100%) and micro (100.00%).

Respondents were also asked to indicate **what would be the categories of risk that a risk-based methodology should take into account when hardware and software manufacturers would be required to demonstrate their compliance with cybersecurity requirements**. A large majority of responses (87%) indicated that a risk-based methodology should include 'the intended use of a product (such as for the provision of health services, as an industrial control system or in a safety context)'. A slightly lower share of responses (83%) also indicated that the methodology should include 'the functionality of a product (such as whether it has a network interface or not, or whether it controls certain security features of a digital system)'. On the other hand, only 44% of responses stressed the need to include 'the societal importance of a product (for example measured in market share or number of users)'.

Similarly, companies of all sizes prioritise the functionality and the intended use of a product.

Within the responses received from respondents who wished to elaborate, it was observed that several respondents expressed their concerns about the definition of high-risk categories or their view that a case-by-case analysis would be more appropriate.

Other respondents raised new aspects that should also be taken into account when developing risk methodologies: a potential stricter process of demonstrating conformity should take into consideration the respective sector in which the product is to be deployed; not only the vulnerability itself but also the exploitability is important. Hence, market share and the number of users counts; the impact of a product on the continuity of the operation (i.a. how deeply it is intertwined with other systems) should also be taken into account; the New Legislative Framework (NLF) has proven to be highly effective in addressing different risk levels of products, e.g. with different modules provided as the basis for conformity assessment procedures and determination of the appropriate risk. This should be applied in the same way in the case of cybersecurity; the larger the market

share, the greater the range for cyber attacks (potential victims); the risks to rights and freedoms of individuals (not covered by the "societal importance" risk category above).

Respondents were asked **who should determine the risk associated with a product and, as a result, its risk categorisation**. The majority of respondents (52%) indicated that risks and risks categorisation should be determined by 'an independent body responsible for verifying compliance with the cybersecurity requirements' while 'a competent authority' was indicated by 39% of respondents.

Similarly, most companies of all sizes chose the same answer, in addition to indicating that manufacturers should also be involved.

Among the respondents who chose to elaborate their answer or to provide a different answer, a few indicated other actors that should be involved in the determination of risk and risk categorisation: an independent body responsible for standardisation like ISO IEC for critical components; the user/customer; the risk associated with a product and, as a result, its risk categorization should be developed jointly in a multi-stakeholder approach.

Q19: Self-declaration

Respondents were asked to assess **if a self-declaration of conformity by a hardware or software manufacturer gives sufficient confidence that security requirements are met** (on a scale from 1 to 5 with 5 indicating that you strongly agree). Most of all respondents responded with 2 (28%), followed by 3 (23%). The response from companies was more positive, with 27% choosing 3, and 23% responding 5.

Most large companies responded with 3 (33%), followed by 2 (19%), and medium companies with 2 (33%). Small companies were equally split between 1 and 5 (40% each), while the two Micro companies were between 2 and 5.

Q20: Third-party verification

Respondents were **asked if they consider that self-declaration is not enough to demonstrate compliance with security requirements, do they think that the involvement of a third party should be required under certain circumstances**. Most respondents answered yes (79%), 13% answered no, while 8% didn't know. There was no difference between the respondent groups.

The majority of large (83%), medium (80%), small (100%) and micro (100%) companies also answered yes.

Respondents were asked **under which circumstances should third-party verification apply**. Most respondents answered that if a product presents a higher risk (68%).

The majority of large (63%), medium (50%), small (100%) and micro (100%) companies agreed.

Those that responded "other" were asked to elaborate. While some respondents thought that self-assessment can be sufficient (in combination with standards, market surveillance and the disciplining effect of the market), nevertheless clear majority said that third-party verification is needed, especially for higher-risk products to ensure compliance, objectivity and accountability.

Q21: Effectiveness of horizontal requirements

Respondents were asked to what extent they agree **that cyber risks can propagate across borders and sectors at high speed, which is why cybersecurity rules for products with digital elements should be aligned at the Union level**. Most respondents strongly agreed (71%) and agreed (21%). There was no difference among the respondent types.

The majority of large (70%), medium (83%), small (60%) and micro (100%) companies also strongly agreed.

Respondents were asked to what extent they agree that **horizontal cybersecurity requirements for products with digital elements would increase the awareness of users when it comes to cyber risks**. Most respondents agreed (54%) and strongly agreed (24). There was no difference among the respondent types.

Large companies agreed (51%) and strongly agreed (24%). Medium companies strongly agreed (50%). 40% of small companies disagreed, while the rest of the responses were split between all the other responses. 100% of Micro companies strongly agreed.

Respondents were asked to what extent they agree **that horizontal cybersecurity requirements for products with digital elements would enhance and ensure a consistently high level of the security of products with digital elements**. Most respondents agreed (43%) and strongly agreed (42%). There was no difference among the respondent types.

Large companies strongly agreed (45%) and agreed (33%). Medium companies strongly agreed (67%). Small companies strongly agreed (40%) and agreed (20%). Micro companies strongly agreed (100%).

Respondents were asked to what extent they agree that **horizontal cybersecurity requirements would improve the functioning of the internal market by levelling the playing field for manufacturers of products with digital elements as regards cybersecurity features**. Most respondents strongly agreed (47%) and agreed (34%). There was no difference among the respondent types.

Large companies agreed (40%) and strongly agreed (36%) Medium companies strongly agreed (67%). Small companies were split between strongly agreeing (40%) and strongly disagreeing (40%). Micro companies strongly agreed (100%).

Q22: Horizontal requirements for digital dual-use products

The EU Action Plan on synergies between civil, defence and space industries underlines the importance of promoting and applying common standards across sectors and the increased relevance of products with digital elements that are used both in a civilian and military context (‘dual-use products’).

Respondents were asked **to what extent could horizontal requirements applying to digital dual-use products contribute to moving the security performance of such products closer to the needs of the defence community and to raising the overall level of cybersecurity in civilian uses** (on a scale from 1 to 5 with 5 indicating a very positive contribution). Most respondents did not know/had no opinion (47%). Among those who had, most selected 4 and 5 (16% each).

Large companies didn’t know/had no opinion (48%), followed by 4 (17%). Medium companies chose 4 and 5 (33% each). Small companies indicated 3 (50%), and the rest were split between 2 and 5 (25% each). Micro companies were split between 1 and 5.

Respondents were asked to elaborate. Some respondents with caveats, but **in general agreed with the question**. Some expressed **scepticism and stressed the differences between the sectors, differing security requirements and potential price increases for consumers**.

Q23: The impact on costs

Respondents were asked to assess the impact of **guidelines or recommendations for the development of secure products with digital elements issued at the EU level addressed to manufacturers** on their costs (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly). Most large companies (49%) responded that the impact on costs will be 2. The responses from medium companies were mixed and equally distributed across 1 and 5 (20%). Most small companies (40%) responded that the impact on costs will be 4. The response from two Micro companies was mixed, equally distributed between 1 and 5.

Respondents were asked to assess the impact of **further voluntary European cybersecurity certification schemes for products with digital elements and services** on their costs (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly). The majority of large (47%), medium (60%) and small (40%) companies responded that the impact on costs will be 3. The response from two micro companies was mixed, equally distributed between 2 and 5.

Respondents were asked to assess the impact of **EU public procurement guidelines taking into account cybersecurity requirements** on their costs (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly). Most large companies (28%) responded 2. Most medium companies (60%) responded 3. Small companies were divided between 2 (40%) and 3 (40%), while two micro companies were between 1 and 5.

Respondents were asked to assess the impact of **amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)** on their costs (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly). Companies of all sizes provided equally split responses, with large companies between 4 (28%) and "Don't know/no opinion" (28%), medium companies between 3 (40%) and 5 (40%), small companies between 1 (40%) and "Don't know/no opinion" (40%), and two micro companies between 1 and 5.

Respondents were asked to assess the impact of **introducing mandatory horizontal cybersecurity requirements for hardware products** on their costs (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly). Large companies' responses closely clustered around 3 (26%) and 4 (23%). Most medium companies responded with 3 (40%), while most small companies indicated 1 (40%). Two micro companies were split equally between 1 and 5.

Respondents were asked to assess the impact of **introducing mandatory horizontal cybersecurity requirements for software products** on their costs (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly). Large companies responded closely between 3 (26%), 4 (23%), 5 (25%). Medium companies were split between 3 (40%) and 5 (40%). Most small companies responded with 1 (40%), while two micro companies were split between 2 and 5.

Respondents were asked to elaborate on their answers, by quantifying the costs if possible. Multiple respondents noted that it is **difficult to quantify and provide costs**.

Several respondents noted that the **benefits will likely outweigh the costs**. Most stakeholders who provided written responses expressed overall **support for the horizontal requirements**. Conversely, multiple stakeholders expressed the **dangers of legislative fragmentation**.

Q24: Proportionate obligations for SMEs

Respondents were asked **if subjecting SMEs to the same obligations as larger companies would ensure that SME hardware and software manufacturers, including individual entrepreneurs, are subject to proportionate obligations (balance between administrative burden and compliance costs on the one hand and a high level of cybersecurity on the other hand) under European legislation introducing mandatory horizontal cybersecurity requirements** (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement). Large companies responded with 4 (30%) and 5 (21%). Most medium and small companies chose 5 (40% within each size category). Two micro companies were split between 4 and 5.

Respondents were asked **if introducing simplified procedures to demonstrate conformity for SMEs and individual entrepreneurs would ensure that SME hardware and software manufacturers, including individual entrepreneurs, are subject to proportionate obligations (balance between administrative burden and compliance costs on the one hand and a high level of cybersecurity on the other hand) under European legislation introducing mandatory horizontal cybersecurity requirements** (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement). Most large companies responded with 4 (24%) and 3 (20%). Medium companies were equally divided between all 5 responses (17% per each response). Small companies were divided between 2 and 5 (20% per response). Two micro companies chose 5.

Respondents were asked to elaborate on which other approaches could ensure proportionate obligations vis-à-vis SME hardware and software manufacturers, including individual entrepreneurs. Several respondents suggested reducing the cost of/simplifying assessment and certification. Several respondents stressed that obligations should be based on the criticality of the product rather than the company size. Several respondents discussed horizontal regulation as a solution.

Q25: The impact on competition

Respondents were asked **if mandatory cybersecurity requirements will put smaller hardware and software manufacturers at a disadvantage compared with larger competitors** (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement). Large companies responded 4 (30%) and 2 (23%). Medium companies were split between 1 and 2 (30% per response). Most small companies chose 1. Two micro companies were split between 2 and 5.

Respondents were asked **if mandatory cybersecurity requirements will put EU hardware and software manufacturers at a disadvantage in the non-EU markets compared to non-EU competitors that are not subject to such requirements** (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement). Large companies chose 2 (33%) and 1 (21%). Most medium companies responded 2 (50%). Small companies we divided between 1 and 3 (40% each), while two Micro companies between 1 and 5.

Q26: The impact on fundamental rights

Respondents were asked **if horizontal cybersecurity requirements for products with digital elements would enhance the protection of privacy and personal data** (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement). Most respondents selected 5 (41%), followed by 4 (32%). There were no outliers among the different types of respondents. Large companies chose 5 (42%) and 4 (33%). Medium companies selected 5 (50%) and 3 (33%). Small companies indicated 3 (40%) and the rest were split between 4 and 5 (20% each). Micro companies chose 5 (100%).

Respondents were asked **if horizontal cybersecurity requirements for products with digital elements would ensure a high level of consumer protection** (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement). Most respondents chose 4 (38%), followed by 5 (36%). There were no outliers among the different types of respondents. Large companies chose 5 (42%) and 4 (35%). Medium companies selected 5 (65%). Small companies indicated 3 (40%) and the rest were split between 4 and 5 (20% each). Micro companies chose 5 (100%).

Q27: Other challenges

Respondents were asked to elaborate if in addition to the issues above, are there other cybersecurity-related challenges not directly linked to the cybersecurity of products that the Cyber Resilience Act should include to enhance the cyber resilience of the internal market. Multiple stakeholders stressed end-user education/responsibility, digital literacy, skills and training. Multiple respondents discussed the need to ensure legislative coherence and avoid duplication and fragmentation. Related to this, some respondents want to narrow the scope of the CRA. Several respondents discussed sector-specific solutions.

ANNEX 3: WHO IS AFFECTED AND HOW?

The following stakeholders would be mainly affected by the initiative:

- Software manufacturers
- Hardware manufacturers
- Importers of products with digital elements
- Distributers of products with digital elements
- End-users, including businesses, public authorities and consumers
- Market surveillance authorities
- Accreditation and notifying authorities
- Notified bodies

The initiative would broadly and most significantly impact the EU software and hardware market. A high-level market overview has been provided in *section 5.1.1*. This Annex includes a more a detailed overview of the **market players** that would be affected by the initiative developed by the supporting study[3], and the **overview of aggregated costs and benefits for the preferred policy option**.

1. Market Analysis: hardware and software manufacturers

The EU software market

Methodology

Based on the data gathered by a recent study which provided for a breakdown of the software and software-based services market,[4] the following categories can be identified: (1) **Software products**;[5] (2) **Software-related services**;[6] (3) **Cloud computing**;[7] (4) **Games.**

[3] Second Interim Study Report N° 2019-0024 supporting the impact assessment
[4] https://op.europa.eu/en/publication-detail/-/publication/480eff53-0495-11e7-8a35-01aa75ed71a1
[5] including infrastructure software & platforms, application software products; excluding SaaS.
[6] including application-related project services, application management, application hosting, infrastructure-related project services, infrastructure outsourcing; excluding cloud services.
[7] paid web-based services consisting of IaaS, PaaS, SaaS.

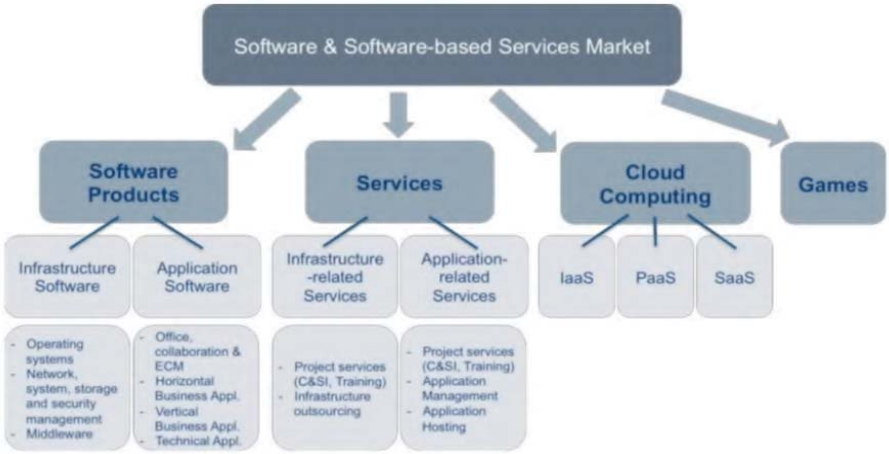


Figure 3: Software market segmentation[8]

The proxy used (**Software Development - SD**) is not an official Eurostat statistic but represents an indicator built for the purpose of this impact assessment. It aims to provide an estimation of the size of the market and is based on the following NACE 2 activities:[9] [J582] Software publishing, which encompasses; [J5821] Publishing of computer games; [J5829] Other software publishing, and [J6201] Computer programming activities. It is worth noting that the data included in this proxy indicator **excludes** activities linked to consultancy activities ([J6202]) facilities management activities ([J6203]) and other information technology and computer service activities ([J6209]) in line with the scope of the initiative.

The software market in Europe has been growing steadily. Due to constraints of available data, the analysis has been narrowed down by looking at a set of six Member States[10] for which complete data was available. Hence, considering a sub-set of EU Member States, the **SD appears to be growing in all its main indicators** (i.e. production value, turnover and total number of enterprises) over the past five year.[11] While production value and turnover increased of 36 % and 39 % respectively, the number of enterprises in the sector experienced a prominent growth, equal to approximately 44 %.

[8] Pierre Audoin Consultants (PAC) GmbH et al (2017): "The Economic and Social Impact of Software & Services on Competitiveness and Innovation (SMART 2015/0015)", *A study prepared for the European Commission*, p. 26.
[9] Indicator elaborated by the Second Interim Study Report N° 2019-0024 supporting the impact assessment.
[10] As the database contains several breaks in the time series of the abovementioned indicators, as well as confidential data for some of the Member States (CZ, DE, FR, IT, HU, PL),
[11] Please note that the following filters were applied when selecting the Member States (2019 values): production value ≥ EUR 10 000 million; turnover ≥ EUR 10 000 million and; enterprises ≥ 15 000 in 2019. This allowed the Project Team to focus on the most robust data entry points. Furthermore, Member States that passed the thresholds but had breaks in the time series were also discarded.

Year	2015	2016	2017	2018	2019
Czech Republic	51 669	55 637	61 157	68 229	72 712
Germany	867	11 793	12 705	13 889	14 874
France	20 868	23 131	23 894	24 797	26 816
Italy	19 359	20 157	20 784	20 773	20 384
Hungary	7 094	7 593	8 647	10 320	11 755
Poland	24 141	23 266	21 954	23 525	25 547
TOTAL	**124 000**	**141 577**	**149 141**	**161 533**	**172 088**

Table 14: SD by country – turnover between 2015 and 2019 in EUR million[12]

The Project Team aggregated the statistics provided by Eurostat concerning the structure of the industry by employment class size in order to assess **the presence of SMEs within the software market**. Due to confidentiality, data is not available for all the Member States, therefore the Project Team has selected a sample of countries[13] with full datasets to assess the proportion of SMEs within the software market. Additionally it is worth noting that the data presented in *Table* constitutes an **over-estimation of the number of enterprises** as the granularity level available in the dataset does not encompass [J6201] as an indicator but provides the aggregated [J620] which also includes computer consultancy activities ([J6202]), computer facilities management activities ([J6203]) and other information technology and computer service activities ([J6209]).

The results illustrate that the software industry is almost entirely composed of SMEs. In fact, whereas the total number of enterprises for the selected sample amounted to 341 781 in 2019, the number of SME operating in the software market in the same year (*Table*) reached 340 918, accounting for 99.7 % of the total. The very large majority (94 %) of SMEs operating in the software market are micro enterprises (less than nine employee). SMEs account for 5 % and 1 % of the market respectively, both relatively more present in the software publishing activity, accounting for a cumulative 11.7 % of total SMEs. However, when looking at the turnover generated by SMEs (*Table*) in the software market for sample countries, it accounts for 41 % of the EUR 305 444 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.

SME size (n° of employees)	All	Micro (0-9)	Small (10-49)	Medium (50-249)
[J582] Software publishing	14 379	12693	1 326	360
[J620] Computer programming, consultancy and related activities	326 539	307 667	15 648	3 224
Total	**340 918**	**320 360**	**16 974**	**3 584**
% of SMEs	**100 %**	**94 %**	**5 %**	**1 %**

Table 15: SD in sample EU countries – number of SMEs in 2019[14]

[12] EUROSTAT [SBS_NA_1A_SE_R2]
[13] Please, note that the Project Team applied the following filters when selecting the Member States (2019 values): total number of enterprise for each indicator ≥ 1000. Furthermore, Member States that passed the thresholds but had breaks in the time series were also discarded. The final sample includes France, Germany, Poland, Romania and Spain.
[14] EUROSTAT [SBS_SC_1B_SE_R2]

SME size (n° of employees)	All	Micro (0-9)	Small (10-49)	Medium (50-249)
[J582] Software publishing	11 410.8	1 735.7	3 662.4	6 012.7
[J620] Computer programming, consultancy and related activities	113 242.3	35 740.2	34 009.1	43 493
Total	**124 653.1**	**37 475.9**	**37 671.5**	**49 505.7**
% of SMEs	**100 %**	**30 %**	**30 %**	**40 %**

Table 16: SD in sample EU countries – turnover in million in 2019[15]

According to the literature, it is in principle possible to segment the open source software (OSS) market into commercial open source and non-commercial open source. In opposition to its counterpart, commercial open source is defined as "*open source software projects that are owned by a single firm that derives a direct and significant revenue stream from the software*"[16]. However, as it also emerged during the consultations for this study (interviews, workshop), it is difficult to estimate the commercial value of commercial open source software solely. Therefore, the values provided in this *Box* are to be considered at an over-evaluation of the market as it encompasses non-commercial OSS as well.

It is estimated that companies located in the EU **invested around EUR 1 billion in OSS in 2018**, which resulted in an overall impact on the European economy of between EUR 65 and 95 billion according to a DG CNECT study[17]. In the same study, a survey carried on 900 companies revealed that small and micro enterprises can attribute over half their revenues to OSS, and particularly OSS related services. Respondents (and particularly small and micro respondents) also reported a high percentage of innovation-related expenses, and almost 50 % of their OSS contributions related to internal product development and another 40 % to already existing OSS. When looking at the key actors in the OSS market, EU OSS manufacturers (solo manufacturers, academics, government personnel and employees) contribute significantly to the global OSS ecosystem. However, it is employees of small and very small businesses that are most likely to contribute OSS code ("commits") in the EU, whereas in other markets, such as the US, commits are mostly made by large manufacturers of products with digital elements. European contributors are estimated to be at least 260 000, representing 8 % of the almost 3.1 million EU employees in the computer programming sector in 2018. 50 % of contributors are already within the ICT industry (8 % of all employees participated in OSS development EU-wide).

	2019	2020	Growth
Open Source Software & IT Services market			
Production Value (in million EUR)	5 233	5 684	*8.6 %*
Share in software market	10.30 %	10.70 %	-
Employment (FTEs)	52 400	56 700	*8.2 %*
Zoom into Open Source Software production values (in EUR million)			

[15] EUROSTAT [SBS_SC_1B_SE_R2]

[16] Riehle, D. (2009). The Commercial Open Source Business Model. In: Nelson, M.L., Shaw, M.J., Strader, T.J. (eds) Value Creation in E-Business Management. AMCIS 2009. Lecture Notes in Business Information Processing, vol 36. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03132-8_2

[17] European Commission, Directorate-General for Communications Networks, Content and Technology, Blind, K., Pätsch, S., Muto, S., et al. (2021) The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy: final study report. Publications Office. https://data.europa.eu/doi/10.2759/430161. The analysis estimates a cost-benefit ratio of above 1:4 and predicts that an increase of 10% of OSS contributions would annually generate an additional 0.4% to 0.6% GDP as well as more than 600 additional ICT start-ups in the EU, p. 14.

Open Source Software	365	403	*10.4 %*
Infrastructure Software & Platforms	199	229	*15.1 %*
Application Software Products	129	138	*7.0 %*
SaaS	27	36	*33.3 %*

Table 17: A closer look at the OSS market in France[18]

As a representation of the growth of the OSS market in the Member States, *Table 17* above includes key metrics to assess the size and growth of such a market in a sample country (France). The data shows a rapid growth of OSS in France, a growth that is assessed as slightly higher than the overall software market, as the market share of OSS & IT services is estimated to have grown by 0.4 percentage points between 2019 and 2020. Similarly, when looking more closely to software available as OSS, a vast majority both in terms of production and growth is carried by infrastructure software and platforms, followed by application software products. Open Source Software as a Service (SaaS) remains a minimal part of the OSS available on the market (8.9 % in 2020) but is the fastest growing market segment (33.3 % from 2019 to 2020).

Box 4: The open source software (OSS) market – outlook

Trends in the EU software market

Along with the rest of the ICT sector, the economic outlook for the software market is positive, having continued to grow throughout the pandemic crisis. Indeed, spending in the software market has seen a year to year growth rate of about 5 % in 2020, a number expected to remain constant in 2021.

As highlighted by the European Parliament in the Global Trends to 2035,[19] the software market will continue evolving with a high reliance on **automation** and **artificial intelligence** in many industries. According to the International Data Corporation (IDC), AI spending is expected to rise by 33 % between 2020 and 2023.

The software market is also impacted by technological advancements such as the surge of **big data** analytics and faster data processing enables business to drive down costs and better define their business strategies by leveraging business intelligence tools and software enabling to make informed decisions based on data (e.g. market trends and consumer buying patterns). The global business intelligence software market size was valued at EUR 23.87 billion in 2018 and is expected to witness a CAGR of 10.1 % from 2019 to 2025.[20]

Trade in EU software market

According to the CN classification, the software is classified according to:[21] *The media on which it's been recorded and the nature of the software. Media include CD, DVD, Laserdisc, Minidisc and other laser-read disks. Even though there are differences in the manufacturing and recording - or writing - processes, these are all designed to be read by some kind of laser system once recorded, floppy disks, magnetic tapes, magnetic stripe cards, memory cards, cartridges for video games consoles. For the purposes of Tariff classification, software categories include: programs and data, sound recordings, computer games, films, pictures and image files, games for video games consoles.*

[18] https://cnll.fr/media/2019_CNLL-Syntec-Systematic-Open-Source-Study.pdf
[19] https://www.oxan.com/media/1969/global-trends-to-2035-geopolitics-and-power.pdf.
[20] Business Intelligence Software Market Size, Share & Trends Analysis Report […], 2019 – 2025. Retrieved from https://www.grandviewresearch.com.
[21] https://trade.ec.europa.eu/access-to-markets/en/content/classifying-computers-and-software

As explained at the beginning of this section, this classification is fully based on products and cannot be directly compared to classifications based on economic activity (e.g. NACE). The latter is at the same time more aggregated, but also better able to reflect the intangible nature of the activities underlying the production of software.

We have then selected the code **8523** (Discs, tapes, solid-state non-volatile storage devices, 'smart cards' and other media for the recording of sound or of other phenomena, whether or not recorded, including matrices and masters for the production of discs) that covers all those software categories.

In percentage terms, compared to hardware, the software share of **extra-EU imports** is lower, and it is separated from that of **intra-EU27 imports** by 18 percentage points (see *Figure 4*). When looking at the figure by country, Ireland (EUR 629 329 645) and the Netherlands (EUR 974 898 158) have higher values of imports from extra-EU27 than intra-EU27. Also, Germany (highest value of extra-EU imports in absolute terms, namely EUR 1 028 886 828), Poland (EUR 584 605 358) and France (EUR 453 722 408) have high values of extra-EU imports, however, for those countries values are lower than intra-EU27 imports.

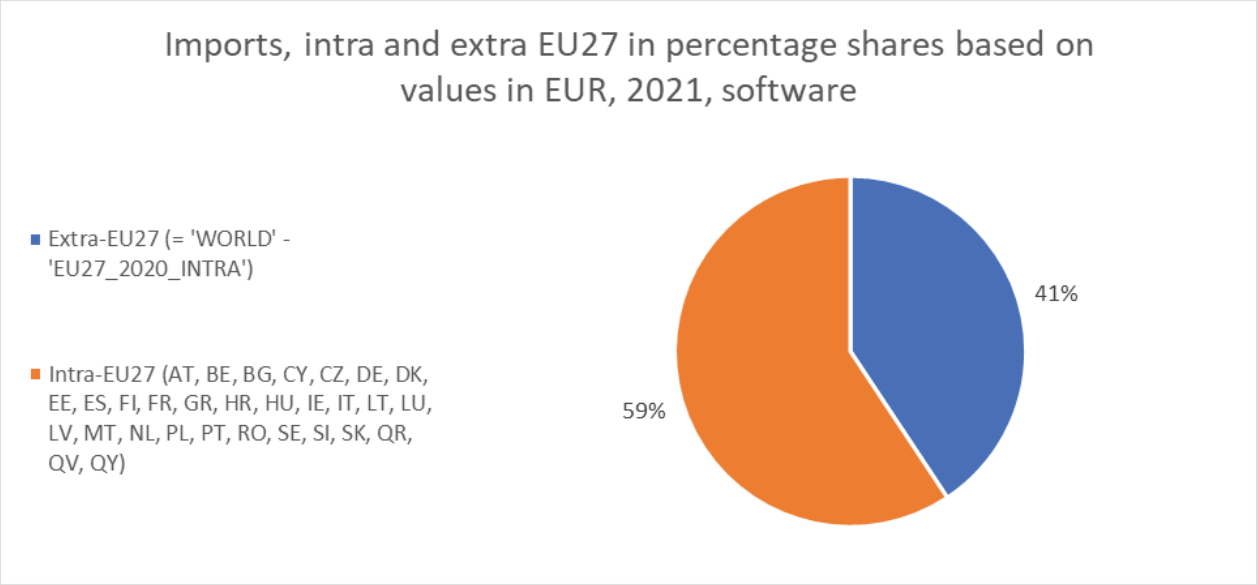


Figure 4: Imports, intra and extra EU27, in percentage shares based on values in EUR, 2021, software[22]

[22] Authors' calculation based on COMEXT – Eurostat

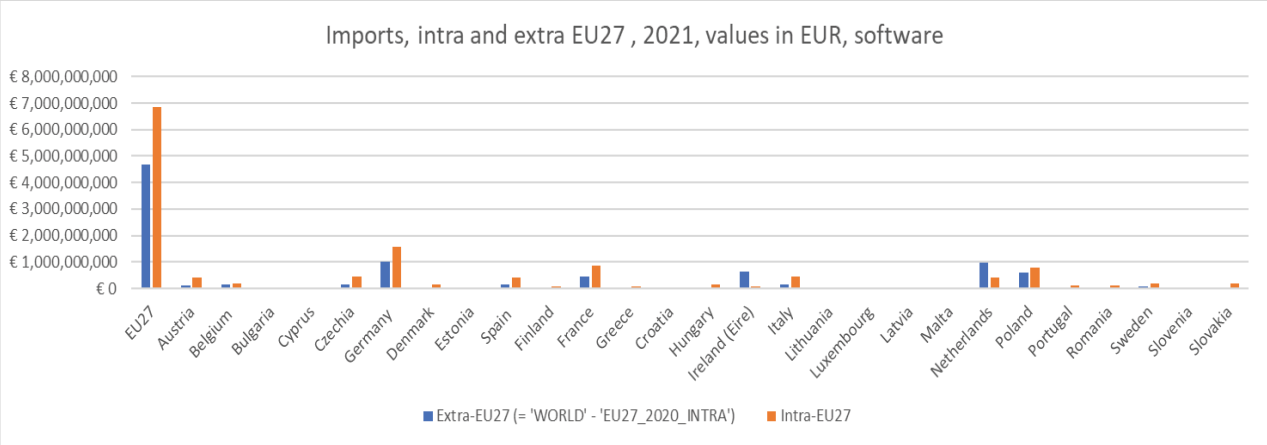


Figure 5: Imports, intra and extra EU27, values in EUR, 2021, software[23]

[23] Authors' calculation based on COMEXT - Eurostat

The EU hardware market

Methodology

Proxies were used to assess the dimension of the hardware market. The data on ICT-SC could be considered as under-representative of the overall market for hardware products as it does not account for manufactured products produced in other sectors (e.g. smart toys), which can be digitally connected. This can lead to an underestimation of impacts. Therefore, the analysis of impacts also considers the extended classification (ICT-EXC-ADJ), representing a sub-set of 2-digit NACE 2 activities of the manufacturing sector combined with a weighting coefficient allowing for a more accurate assessment of the hardware market

The proxies used to provide an estimation of the size of the market are:

1. ICT manufacturing sector – standard classification (ICT-SC), representing a sub-set of 3-digit NACE 2 activities of the manufacturing sector. The ICT-SC is used by Eurostat as standard classification for economic activity. The NACE 2 activities included in the ICT-SC are:
    - [C261] Manufacture of electronic components and boards;
    - [C262] Manufacture of computers and peripheral equipment;
    - [C263] Manufacture of communication equipment;
    - [C264] Manufacture of consumer electronics; and
    - [C268] Manufacture of magnetic and optical media.

    It is worth noting that the data on ICT-SC could be considered as under-representative of the overall market for hardware products as intended by the scope of this study, as it does not account for products manufactured in other sectors (e.g.; smart toys in C324) which can be digitally connected. Nevertheless, at present, ICT-SC appears to be the most appropriate proxy to assess the hardware market as similar classifications are also used in relevant publications.[24]

2. ICT manufacturing sector – extended classification (ICT-EXC), representing a sub-set of 2-digit NACE 2 activities of the manufacturing sector. The ICT-EXC is not an official Eurostat statistic but represents an indicator built by the Project Team for the purpose of this study. The NACE 2 activities included in the ICT-EXC are:
    - [C26] Manufacture of computer, electronic and optical products;
    - [C27] Manufacture of electrical equipment;
    - [C28] Manufacture of machinery and equipment n.e.c.;
    - [C30] Manufacture of other transport equipment;
    - [C32] Other manufacturing; and
    - [C33] Repair and installation of machinery and equipment.

    The ICT-EXC can be considered the upper limit for the assessment of the size of the hardware market. It is worth noting that the ICT-EXC assumes that all the products manufactured in these sectors are digital or feature a digital component. This is indeed a relevant limitation of this approach as it overestimates the size of the hardware market. For this reason, the Project Team

[24] See footnote 140.

applied a weighting coefficient allowing for a more accurate assessment of the hardware market. Particularly, this study applies the percentage of enterprises integrating digital processes to the selected ICT-EXC indicators to all the NACE 2 2-digit activities selected by the Project Team (see above), with the exception of C26 which is considered in its entirety.[25]

The calculation of the different indicators will be performed by using the formula below, providing ICT-EXT adjusted (ADJ) results. The Project Team recognises that the percentage of enterprises integrating digital processes (K in the formula below) represents a sub-optimal coefficient as it does not refer to the production of products with digital elements within the sectors, but to measures of digital intensity within the production process. This happens because the NACE classification is 'economic activity-based', and not 'product-based' classification. As the coefficient differs for each NACE 2 activity, *Table 9* presents the coefficient applied to each activity for the purpose of this study. Hence, the parameters of the NACE 2 activities are adjusted by multiplying the total value with the coefficients of *Table 19*.

$$ICT\text{-}EXT\text{-}ADJ\ indicator = C26 * K^{C26} + C27 * K^{C27} + C28 * K^{C28} + C30 * K^{C30} + C32 * K^{C32} + C32 * K^{C32}$$

Table 18 shows the NACE 2 activities included by the Project Team in the different proxies used to assess the hardware market.

[25] 'C26 Manufacture of computer, electronic and optical products' represents the core ICT sector as defined by Eurostat. Hence, as for the calculation of the market size for ICT-SC, the Project Team will consider it in its entirety so to be able to apply the coefficient at the same NACE 2 (2-digit) level. The coefficients for the percentage of enterprises integrating digital processes are not available at NACE 2 3-digit level.

Code	Type of NACE 2 economic activity	ICT-SC	ICT-EXC
26	Manufacture of computer, electronic and optical products		
261	Manufacture of electronic components and boards	x	x
262	Manufacture of computers and peripheral equipment	x	x
263	Manufacture of communication equipment	x	x
264	Manufacture of consumer electronics	x	x
265	Manufacture of instruments and appliances for measuring, testing and navigation; watches and clocks		x
266	Manufacture of irradiation, electromedical and electrotherapeutic equipment		x
267	Manufacture of optical instruments and photographic equipment		x
268	Manufacture of magnetic and optical media	x	x
27	Manufacture of electrical equipment		
271	Manufacture of electric motors, generators, transformers and electricity distribution and control apparatus		x
272	Manufacture of batteries and accumulators		x
273	Manufacture of wiring and wiring devices		x
274	Manufacture of electric lighting equipment		x
275	Manufacture of domestic appliances		x
279	Manufacture of other electrical equipment		x
28	Manufacture of machinery and equipment n.e.c.		
281	Manufacture of general — purpose machinery		x
282	Manufacture of other general-purpose machinery		x
283	Manufacture of agricultural and forestry machinery		x
284	Manufacture of metal forming machinery and machine tools		x
289	Manufacture of other special-purpose machinery		x
30	Manufacture of other transport equipment		
301	Building of ships and boats		x
302	Manufacture of railway locomotives and rolling stock		x
303	Manufacture of air and spacecraft and related machinery		x
304	Manufacture of military fighting vehicles		x
309	Manufacture of transport equipment n.e.c		x
32	Other manufacturing		
321	Manufacture of jewellery, bijouterie and related articles		x
322	Manufacture of musical instruments		x
323	Manufacture of sports goods		x
324	Manufacture of games and toys		x
325	Manufacture of medical and dental instruments and supplies		x
329	Manufacturing n.e.c.		x
33	Repair and installation of machinery and equipment		
331	Repair of fabricated metal products, machinery and equipment		x
332	Installation of industrial machinery and equipment		x

Table 18: Proxies and NACE 2 activities[26]

[26] European Commission Digital Economy and Society Index (DESI)

Code	Type of NACE 2 economic activity	Share enterprises digital processes (2019)
26	Manufacture of computer, electronic and optical products	1[1]
27	Manufacture of electrical equipment	63%
28	Manufacture of machinery and equipment n.e.c.	60%
30	Manufacture of other transport equipment	60%
32	Other manufacturing	40%
33	Repair and installation of machinery and equipment	40%

Table 19: Share of enterprises implementing digital processes by NACE2 activity – ICT-EXT-ADJ[27]

ICT manufacturing sector – standard classification

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[28] with a total **number of enterprises** of 22 773.[29]

As the database contains several breaks in the time series of the abovementioned indicators, the Project Team narrowed down the analysis by looking at a set of six Member States for which complete data was available. Hence, considering a sub-set of EU Member States, the ICT-SC appears to be growing in all its main indicators (i.e.; production value, turnover and total number of enterprises) over the past five year.[30] *Table* , *Table* and *Table* illustrate the upward trend over time of these indicators in the selected countries. Particularly, while production value and turnover increased of 21 % and 23 % respectively between 2015 and 2019, the number of enterprises in the sector experienced a less prominent growth, equal to approximately 13 % over the same reference period.

Year	2015	2016	2017	2018	2019
Czech Republic	8 071.5	8 193.4	8 351.8	9 676.7	9 427.7
Germany	33 698.4	33 270.9	33 069.9	34 186.6	34 841.1
France	16 067.5	16 487.5	14 895.8	22 653.9	26 720.1
Italy	10 382.7	10 695.5	10 927.5	11 720.1	12 087.0
Hungary	9 540.3	9 908.3	10 596.7	10 174.7	12 320.2
Poland	7 608.5	7 101.0	7 805.9	8 110.9	8 042.4
TOTAL	**85 368.9**	**85 656.6**	**85 647.6**	**96 522.9**	**103 438.5**

Table 20: ICT-SC by country - production value between 2015 and 2019 in EUR million[31]

[27] European Commission Digital Economy and Society Index (DESI)
[28] 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
[29] EUROSTAT. Annual enterprise statistics for special aggregates of activities (NACE Rev. 2). [SBS_NA_SCA_R2]
[30] Please note that the Project Team applied the following filters when selecting the Member States (2019 values): production value ≥ EUR 8 000 million; turnover ≥ EUR 8 000 million and; enterprises ≥ 1 000 in 2019. This allowed the Project Team to focus on the most robust data entry points. Furthermore, Member States that passed the thresholds but had breaks in the time series were also discarded.
[31] EUROSTAT [SBS_NA_SCA_R2]

Year	2015	2016	2017	2018	2019
Czech Republic	8 315.1	8 391.6	8 860.9	10 190.8	9 956.7
Germany	37 761.7	37 459.8	37 671.6	43 272.4	41 746.9
France	16 792.0	17 439.5	15 387.2	23 585.0	27 364.9
Italy	10 495.0	10 770.6	11 093.8	11 293.2	11 678.3
Hungary	10 939.4	11 453.1	12 113.0	11 491.5	14 143.9
Poland	8 127.0	7 675.4	8 207.4	8 981.8	8 895.9
TOTAL	**92 430.2**	**93 190.0**	**93 333.9**	**108 814.7**	**113 786.6**

Table 21: ICT-SC by country - turnover between 2015 and 2019 in EUR million[32]

Year	2015	2016	2017	2018	2019
Czech Republic	2 348	2 326	2 303	2 238	2 260
Germany	3 762	3 684	3 644	4 275	4 423
France	1 693	1 632	1 381	1 417	1 416
Italy	3 370	3 327	3 265	3 204	3 303
Netherlands	919	909	926	1 015	1 050
Poland	1 738	1 896	2 019	2 428	2 448
Slovakia	621	920	974	1 388	1 414
TOTAL	**14 451**	**14 694**	**14 512**	**15 965**	**16 314**

Table 22: ICT-SC by country - number of enterprises between 2015 and 2019[33]

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 are equally split between 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. This represents an important distinction with the software and services market where the B2B component is predominant, accounting for more than two-thirds of the overall sales.[34]

The device market – outlook[35]

The device market is a segment of the IT hardware market, including PCs and phones sub-segments. While the PCs' segment encompasses physical units of computing systems (e.g.; tablets), the phones' segment includes mobiles and fixed lines used both by businesses and consumers. The global revenues of the device market amounted to **EUR 766 billion in 2021**, with Europe accounting for 24 % of the total (**EUR 184 billion**).[36]

The phones' segment represents the most relevant part of the device market with a total revenue of EUR 511 million in 2021 and expected to reach EUR 586 billion by 2026 (CAGR equal to 2.8 %). The European phones' market accounts for 23 % of the total in 2021 (**EUR 117 billion)**, with Germany and France being the two main markets (EUR 17 and 12 billion respectively)[37].

The PC' segment reached global revenues for EUR 255 billion in 2021, with Europe accounting for 26 % of the total (**EUR 66 billion**). The segment is expected to have a

[32] EUROSTAT [SBS_NA_SCA_R2]
[33] EUROSTAT [SBS_NA_SCA_R2]
[34] Deloitte (2019). The German Technology Sector. From Hardware to Software & Services. p. 12
[35] Statista (2021). Devices Report 2021 -Statista Technology Market Outlook. December 2021.
[36] Currency exchange rate EUR/USD on 16/05/2022.
[37] Currency exchange rate on 06/05/2022

slower growth than the phones' segment as the CAGR is expected to be 0.9 % until 2026.

The Project Team aggregated the statistics provided by Eurostat concerning the structure of the industry by employment class size to assess **the presence of SMEs within the hardware market**. The results illustrate that the European ICT-SC manufacturing industry is almost entirely composed of SMEs. In fact, whereas the total number of enterprises amounted to 22 773 in 2019, the number of SME operating in the hardware market in the same year reached 22 119, accounting for 97.13 % of the total. The large majority (82 %) of SMEs operating in the hardware market are micro enterprises (less than nine employee). SMEs account for 14 % and 4 % of the market respectively, the latter being relatively more present in the manufacturing of electronic components and boards, amounting to 5.7 % of the total SMEs. 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.

SME size (n° of employees)	All	Micro (0-9)	Small (10-49)	Medium (50-249)
Manufacture of electronic components and boards (C261)	9 669	7 333	1 781	555
Manufacture of computers and peripheral equipment (C262)	5 347	4 745	462	140
Manufacture of communication equipment (C263)	4 629	3 815	591	223
Manufacture of consumer electronics (C264)	2 462	2 201	198	63
Manufacture of magnetic and optical media (C268)	12	*NA*	12	*NA*
Total	**22 119**	**18 094**	**3 044**	**981**
% SMEs	**100 %**	**82 %**	**14 %**	**4 %**

Table 23: ICT-SC in EU-27 - number of SMEs in 2019 by size[38]

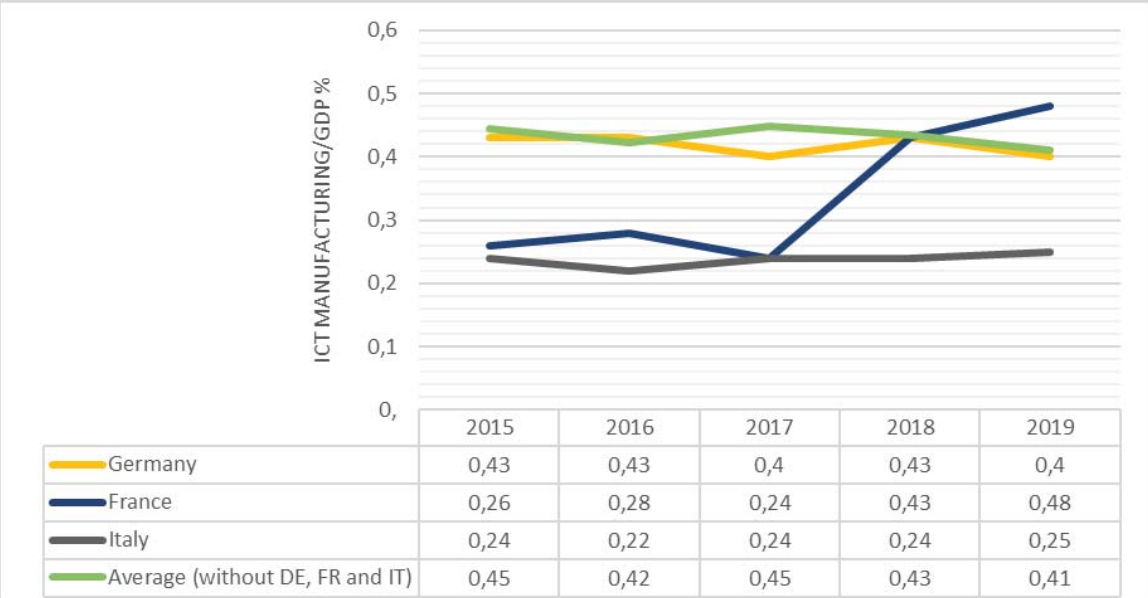
SME size (n° of employees)	All	Micro (0-9)	Small (10-49)	Medium (50-249)
Manufacture of electronic components and boards (C261)	19 071.7	2 346.0	5 357.8	11 367.9
Manufacture of computers and peripheral equipment (C262)	3 263.7	1 240.4	2 023.3	*NA*
Manufacture of communication equipment (C263)	9 234.0	1 784.4	1 942.1	5 507.5
Manufacture of consumer electronics (C264)	2 595.8	325.4	725.2	1 545.2
Manufacture of magnetic and optical media (C268)	86.3	33.4	52.9	*NA*
Total	**34 251.5**	**5 729.6**	**10 101.3**	**18 420.6**
% SMEs	**100 %**	**82 %**	**14 %**	**4 %**

Table 24: ICT-SC in EU-27 – turnover in EUR million in 2019 by size[39]

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.[40] *Figure 6* presents the evolution of the relative weight of the ICT-SC on the GDP of the main European economies (i.e.: Germany, France and Italy) between 2015 and 2019.

[38] EUROSTAT [SBS_SC_IND_R2]
[39] EUROSTAT [SBS_SC_IND_R2]
[40] EUROSTAT. Percentage of the ICT sector on GDP. [TIN00074]

While France experienced a substantial increase in the relative weight of the sector, Germany and Italy ICT-SC manufacturing did not change over the period under analysis. Furthermore, the graph outlines the average of the same indicator for a larger set of EU Member States.[41]



	2015	2016	2017	2018	2019
Germany	0,43	0,43	0,4	0,43	0,4
France	0,26	0,28	0,24	0,43	0,48
Italy	0,24	0,22	0,24	0,24	0,25
Average (without DE, FR and IT)	0,45	0,42	0,45	0,43	0,41

Figure 6: Percentage of the ICT-SC on GDP - Value added at factor cost in the ICT-SC sector[42]

In 2018, the **value added** of the ICT sector in the EU-27 amounted to EUR 590 billion. Nevertheless, more than 90 % of the value-added concerns ICT services, with ICT-SC accounting for a marginal part over the total. Moreover, it is important to point out that, while the ICT service sector experienced an upward trend in the value-added between 2006 and 2018, the ICT-SC witnessed a slight decline in the same period.[43] *Figure* 7 presents the value-added trend over between 2006 and 2020 (please note that 2019 and 2020 represent nowcasted data.

[41] Namely the average of Belgium; Bulgaria; Czech Republic; Estonia; Greece; Croatia; Lithuania; Hungary; Austria; Poland; Romania; Slovenia; Slovakia.
[42] EUROSTAT [TIN00074]
[43] European Commission (2021). Digital Economy and Society Index (DESI) 2021, p. 77.

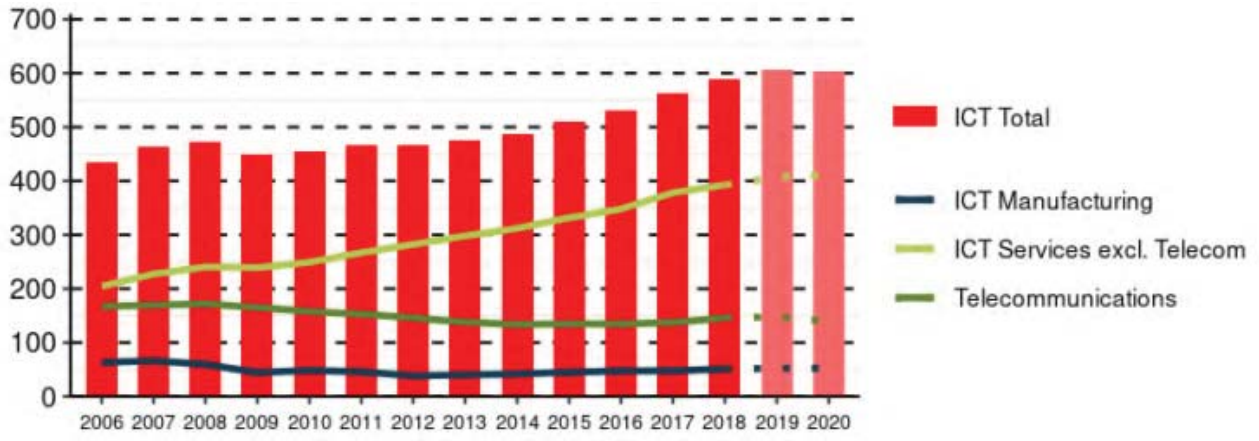


Figure 7: ICT-SC value-added between 2006 and 2020 - EUR billion[44]

ICT manufacturing sector – extended classification

When considering the **ICT-EXT-ADJ**, 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. *Figure 8* provides a breakdown by NACE 2 activities of the estimated market size for hardware in 2019. The manufacture of machinery equipment and n.e.c. represents the main one for production value and turnover. On the contrary, repair and installation of machinery equipment is the NACE 2 activity with the highest number of enterprises.

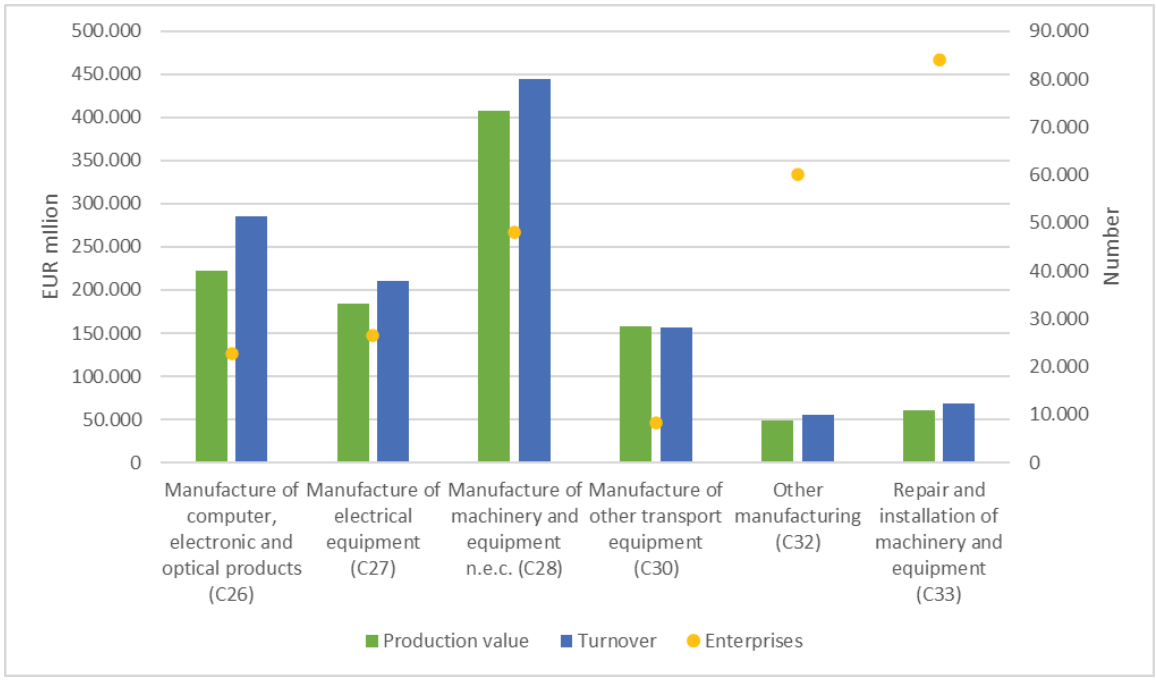


Figure 8: Breakdown of indicators by NACE2 activities (ICT-EXC-ADJ) – EU27, 2019[45]

Semiconductors (also known as chips) are substances that have specific electrical properties allowing them to ensure the conductivity between conductors and insulators,

[44] European Commission (2021). Digital Economy and Society Index (DESI) 2021, p. 77.
[45] Eurostat data.

making them a founding component for computers and other electronic devices. Semiconductors are essential to many commonly used hardware products such as smartphones, tablets or PCs. The European Semiconductor Industry Association (ESIA) reported that **yearly semiconductor sales in the European market reached EUR 44.57 billion in 2021, a 27.3 % increase versus 2020**. As global reliance on electronics continues to grow, the potential market for semiconductor manufacturers and retailers will continue to increase as well. 2022 is expected to reach two-digit growth compared to the previous year, with revenue from sales expected to amount to EUR 49 billion.[4647]

Globally, semiconductor sales amounted to EUR 518.81 billion in 2021, a 26.2 % increase from 2020. Therefore, the European market for semiconductors represented, in 2021, 8.6 % of global sales, a slight increase from the 8.5 % of 2020.[48] However, sales from 2019 to 2020 have seen a slower increase globally and even decreased in Europe as shown below. The lag encountered in the European semiconductor market has been increasingly catching up since 2020 with increasing forecasted sales. This growth in the European market is expected to exceed the global figure with the market share dedicated to European enterprises increasing from year to year.

Semiconductor global and European market outlook[49]

	2019	2020	2021	2022*
Global semiconductor sales (in EUR billion)	384.1	411.1	518.8	560.0
Growth	-	*7 %*	*26 %*	*8 %*
European semiconductor sales (in EUR billion)	37.2	35.0	44.6	49.4
Growth	-	*-6 %*	*27 %*	*11 %*
European market share	9.7 %	8.5 %	8.6 %	8.8 %

**Values for 2022 are forecast estimates*

The sharp increase in demand, fuelled by the effects of the COVID-19 pandemic, over the past three years has lead to a shortage in the supply of semiconductors heavily impacting a variety of industries such as automotive, health, defence or security. This global semiconductor shortage has exposed European dependency on supply from a limited number of companies and geographies, and its vulnerability to third country export restrictions and other disruptions in the present geopolitical context. Therefore, in line with the Commission's objective of creating a state-of-the-art European chip ecosystem[50], the Commission released a proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)[51]. The EU Chips Act proposes to develop a thriving semiconductor ecosystem and resilient supply chain, while setting measures to prepare, anticipate and respond to future supply chain disruptions. To this end, if approved, the European Chips Act will have more than EUR 43 billion in place to support the development of European semiconductor supply chains.

Box 5: The semiconductor market – outlook

Markets trends

[46] Currency exchange rate EUR/USD on 16/05/2022.
[47] Statistics available here.
[48] https://www.eusemiconductors.eu/sites/default/files/ESIA_WSTS_PR_2112.pdf
[49] https://www.statista.com/topics/1182/semiconductors/
[50] State of the Union address 2021. https://ec.europa.eu/info/sites/default/files/soteu_2021_address_en_0.pdf
[51] Chips Act Proposal COM(2022) 46 final..

Despite the impacts of the COVID-19 pandemic, the **IT budget of European companies appears to be growing in 2022,** as outlined by a survey.[52] Particularly, more than half of the sample declared that the IT budget will increase during the year. This trend appears to be more prominent when considering big (more than 500 employees) corporations where two-thirds of the sample signalled its intention to increase the budget. Within the IT budget, hardware represents the **largest share of the spending** (30 % in 2022), especially for SMEs.

While not specific only the hardware market, an important trend concerning hardware is the **continuous growth of the IoT sector**. Particularly, IoT spending will grow at CAGR of 12.32 % from EUR 131 billion in 2019 to EUR 230 billion in 2024.[53] By looking at the application level, the revenue in the European IoT market, including smart home technologies and smart finance technologies but excluding other IoT use cases, is projected to reach EUR 5.04 billion in 2022 and is foreseen to witness an CAGR equal to 10.5 % between 2022 and 2027, resulting in a market volume of EUR 8.14 billion by 2027.[54] Other IoT use cases (e.g.; autonomous cars, industrial IoT) represent more relevant market sub-segments, accounting for EUR 20.17 billion in 2020.[55] It is worth noting that this figure includes software and thus, it is an over-representation of the market segment.

An important trend concerning hardware is the **continuous growth of the IoT market**. The IoT market refers to all internet-enabled objects and devices that collect and exchange data. IoT products include wearables (e.g. smartwatch), smart home devices, security systems, thermostats, intelligent transportation, smart grids, and many more. They may also be referred to as connected things or smart devices. It is possible to define the European IoT market by considering it in three main ways:[56]

- **Infrastructure** – the market is segmented into platform, mobile networks and access technologies, cloud solutions/storage and processing, analytics and security;
- **Vertical** – the market is segmented into healthcare, energy, public & services, transportation, retail, individuals, and others (e.g.; manufacturing); and
- **Application –** the market is segmented into smart home, smart wearable, smart cities, smart grid, IoT industrial internet, IoT connected cars, IoT connected healthcare, and others (e.g..; toys and drones).

The IoT market represents an important part of the hardware market. The European IoT spending is expected to grow rapidly in the upcoming years. Particularly, IoT spending are forecasted to grow at CAGR of 12.32 % from EUR 131 billion in 2019 to EUR 230 billion in 2024.[57] The IoT spending encompasses not only hardware but also connectivity, services and software spending. However, hardware remains the most relevant component of the spending, accounting for a third of the total.
Looking at revenue from the IoT market in Europe, it increased in 2021 to around EUR 4.47 billion, up from around EUR 3.07 billion in 2020.[58] By focusing at the application

[52] https://swzd.com/resources/state-of-it/#soit-2022
[53] Commission (2021). Advanced Technologies for Industry – AT WATCH. Technology Focus on the Internet of Things. March 2021.
[54] https://www.statista.com/outlook/tmo/internet-of-things/europe
[55] https://www.marketwatch.com/press-release/europe-industrial-iot-market-2021-to-2030-new-study-industry-scope-and-growth-strategies-progressing-at-a-cagr-of-107-during-the-forecast-period-2022-02-22
[56] https://www.researchandmarkets.com/reports/5013423/european-iot-market-2019-2025
[57] European Commission (2021). Advanced Technologies for Industry – AT WATCH. Technology Focus on the Internet of Things. March 2021.
[58] Currency exchange rate EUR/USD on 27/05/2022.

level (e.g. smart home, smart wearable, smart cities, smart grid, IoT industrial internet), the revenue in the European IoT market, including smart home technologies and smart finance technologies but excluding other IoT use cases, is projected to reach EUR 5.04 billion in 2022 and is foreseen to witness an annual growth rate (CAGR) equal to 10.5 % between 2022 and 2027, resulting in a market volume of EUR 8.14 billion by 2027.[59] Other IoT use cases (e.g.; autonomous cars, industrial IoT) represent more relevant market sub-segments, accounting for EUR 20.17 billion in 2020.[60] It is worth noting that this figure includes software.

Box 6: The IoT market – outlook

The hardware market is also experiencing **new technological trends such as tinyML and low power wide area network (LPWAN).** These technological developments seek to address the challenges of high operating costs of machine learning and IoT technologies, while increasing the power efficiency of traditional hardware. TinyML is a machine learning technology allowing users to run on-device, local, sensor data analytics at low-latency, low power and low bandwidth. Consequently, TinyML devices can operate ML applications while being unplugged on batteries for long periods of time (i..; in some cases years). This hardware technology is currently being used in several fields of application such as industrial productive maintenance, agriculture, healthcare and maritime conservation. LPWAN represents a set of low-power, long range area network technologies for small sensor-based data. As LPWAN operate with very little data rates and low power, the hardware underlying these systems can be developed at a very low cost. In 2020, the LPWAN market amounted to more than EUR 2.4 billion (with the European market surpassing EUR 575 million) and is expected to grow at a CAGR of over 60% between 2021 and 2027. Particularly, the German market is forecasted at more than EUR 3 billion by 2027 as both the government and the industry renewed their efforts to replace traditional approaches with LPWAN implementations.

Trade in the EU hardware sector

When selecting relevant codes from the CN classification to reflect the size of imports and exports of hardware, the methodological choice has been made to select all codes at 4-digit level (e.g. Electrical machines and apparatus, having individual functions) that classify **computers and computer parts**, as these codes cover for most of the machinery and other types of products such as basic units and components that play a digital function within a product. We are aware that, given the wide range of products and 'smart' products that the legislation could cover, some codes might be left out by this selection. While making the selection of these codes, the 8-digit level was studied too, in order to assess the relevance of including the specific codes or making a choice to exclude them (e.g. in case they refer to purely passive components, for example, code 8524 *Flat panel display modules, whether or not incorporating touch sensitive screens* are excluded because they do not incorporate drivers or circuits). The main codes selected are:

- **8443** Printing machinery used for printing by means of plates, cylinders and other printing components of heading 8442; other printers, copying machines and facsimile machines, whether or not combined; parts and accessories (**note:** codes 8443 31, 8443 32 are particularly relevant for products with digital elements with smart functions as they refer to *Machines which*

[59] https://www.statista.com/outlook/tmo/internet-of-things/europe

[60] https://www.marketwatch.com/press-release/europe-industrial-iot-market-2021-to-2030-new-study-industry-scope-and-growth-strategies-progressing-at-a-cagr-of-107-during-the-forecast-period-2022-02-22

perform two or more of the functions of printing, copying or facsimile transmission, capable of connecting to an automatic data processing machine or to a network and – *Other, capable of connecting to an automatic data-processing machine or to a network*).

- **8471** Automatic data-processing machines and units thereof; magnetic or optical readers, machines for transcribing data onto data media in coded form and machines for processing such data (**note:** all sub-codes are highly relevant for products with digital elements).
- **8473** Parts and accessories (other than covers, carrying cases, and the like) suitable for use solely or principally with machines of headings 8470 Calculating machines and pocket-size data recording, reproducing, and displaying machines with calculating functions, and to 8472 Other office machines (for example, hectograph or stencil duplicating machines, addressing machines, automatic banknote dispensers, coin-sorting machines) **(note**: this code represents all computer parts. There is a code 8542, that refers to electric circuits however, Eurostat does not include this code within the classifications linked to computers, computer parts, and software).
- **8504** Electrical transformers, static converters (for example, rectifiers) and inductors (code 8504 40 30 is – Of a kind used with telecommunication apparatus, automatic data-processing machines and units).
- **8514** Industrial or laboratory electric furnaces and ovens (including those functioning by induction or dielectric loss); other industrial or laboratory equipment for the heat treatment of materials by induction or dielectric loss.
- **8517** Telephone sets, including smartphones and other telephones for cellular networks or for other wireless networks; other apparatus for the transmission or reception of voice, images or other data, including apparatus for communication in a wired or wireless network (such as a local or wide area network), other than transmission or reception apparatus.
- **8518** Microphones and stands therefor; loudspeakers, whether or not mounted in their enclosures; headphones and earphones, whether or not combined with a microphone, and sets consisting of a microphone and one or more loudspeakers; audio-frequency electric amplifiers; electric sound amplifier sets.
- **8519** Sound recording or sound reproducing apparatus.
- **8521** Video recording or reproducing apparatus, whether or not incorporating a video tuner
- **8523** Discs, tapes, solid-state non-volatile storage devices, 'smart cards' and other media for the recording of sound or of other phenomena, whether or not recorded, including matrices and masters for the production of discs, but excluding products of Chapter 37.
- **8525** Transmission apparatus for radiobroadcasting or television, whether or not incorporating reception apparatus or sound recording or reproducing apparatus; television cameras, digital cameras and video camera recorders.
- **8526** Radar apparatus, radio navigational aid apparatus and radio remote control apparatus
- **8527** Reception apparatus for radiobroadcasting, whether or not combined, in the same housing, with sound recording or reproducing apparatus or a clock.
- **8528** Monitors and projectors, not incorporating television reception apparatus; reception apparatus for television, whether or not incorporating

radio-broadcast receivers or sound or video recording or reproducing apparatus.

- **8543** Electrical machines and apparatus, having individual functions.

- **8544** Insulated (including enamelled or anodised) wire, cable (including coaxial cable) and other insulated electric conductors, whether or not fitted with connectors; optical fibre cables, made up of individually sheathed fibres, whether or not assembled with electric conductors or fitted with connectors (note: this code can be spurious, as it can include passive components).

Following the definition, hardware imports from extra-EU countries and intra-EU imports are similar shares, with intra-EU imports only surpassing extra-EU ones by five percentage points (see *Figure 9*). When looking at country by country figures, the value of intra-EU imports is higher than extra-EU ones for most countries with some notable exceptions, namely for the Netherlands (EUR 80 551 944 490, namely EUR 62 381 300 510 higher than intra-EU imports), Ireland (EUR 4 851 072 314, namely EUR 1 958 955 443 higher than intra-EU imports), Hungary (EUR 6 753 493 869, namely EUR 1 031 473 773 higher than intra-EU imports), and the Czech Republic (EUR 16 628 116 800, namely EUR 2 543 176 067 higher than intra-EU imports).

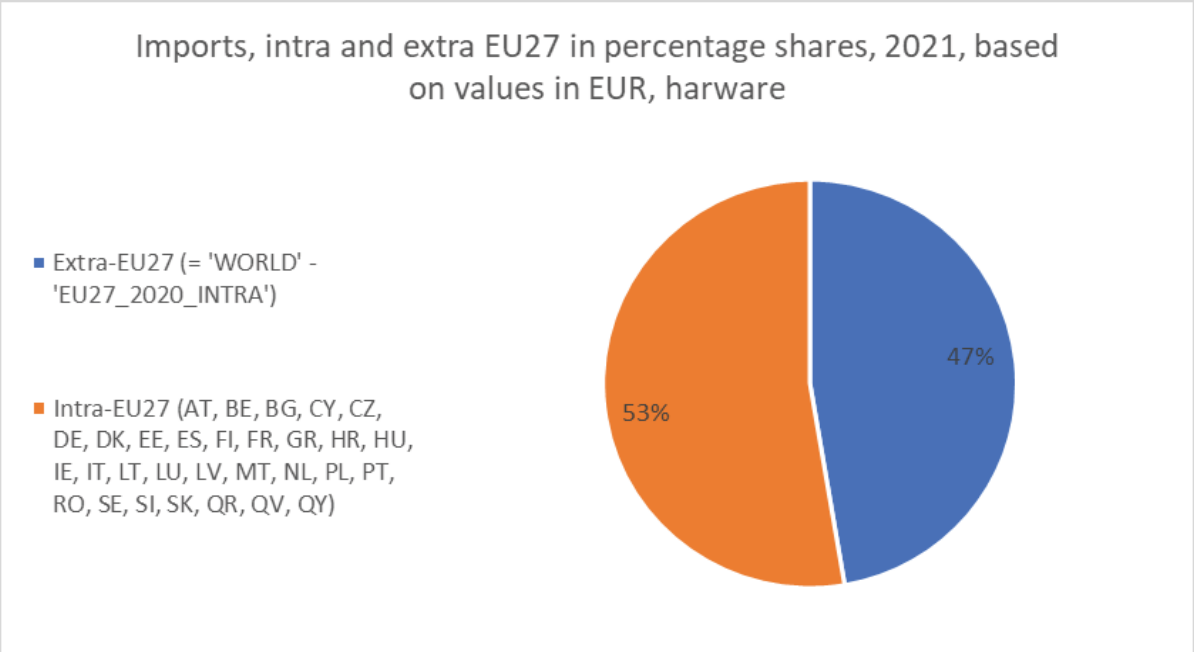


Figure 9: Imports, intra and extra EU27, in percentage shares based on values in EUR, 2021, hardware[61]

[61] Author's calculation based on COMEXT – Eurostat.

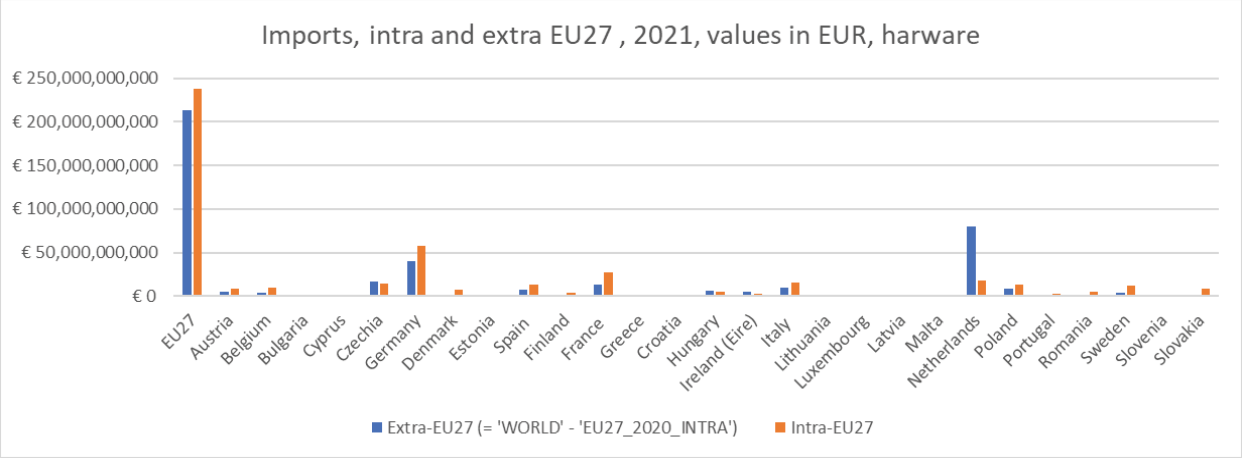


Figure 10: Imports, intra and extra EU27, values in EUR, 2021, hardware[62]

[62] Author's calculation based on COMEXT – Eurostat.

Aggregated market for products with digital elements

The global market for products with digital elements encompassing software and hardware has a total production value in of EUR 458 billion and turnover of EUR 550 billion in 2019,[63] if the hardware market is considered as only including the elements of the ICT-SC indicator. Considering the extended classification (ICT-EXT-ADJ), these values soar to EUR 1317 billion in production value and EUR 1485 billion in turnover for 2019.

The number of enterprises operating in this sector is 388 532 when considering the limited scope of ICT-SC and of 615 272 with a broader scope as defined by the ICT-EXT-ADJ indicator with a vast majority being SMEs according to the Project Team's estimations. Based on this data, these SMEs account for about 34.4 % of the turnover generated in the market for products with digital elements for 2019. *Table 25* and *Table 26* illustrate these statistics.

Indicators	Software (SD)	Hardware (ICT-SC)	Total
Production value (in billion EUR)	236	222	**458**
Turnover (in billion EUR)	265	285	**550**
% from SMEs	*41 %*[64]	*21.90 %*	***34.40 %***
Number of enterprises	365 759	22 773	**388 532**
% from SMEs	*99.70 %*[65]	*97.10 %*	***99.58 %***

Table 25: Aggregated indicators for global market for products with digital elements in 2019 in the EU (SD & ICT-SC)[66]

Indicators	Software (SD)	Hardware (ICT-EXT-ADJ)	Total
Production value (in EUR billion)	236	1 081	**1 317**
Turnover (in EUR billion)	265	1 220	**1 485**
% from SMEs	*41 %*[67]	*21.90 %*	***34.40 %***
Number of enterprises	365 759	249 513	**615 272**
% from SMEs	*99.70 %*[68]	*97.10%*	***99.58 %***

[63] Second Interim Study Report N° 2019-0024 supporting the impact assessment.
[64] Percentage based on sample countries (France, Germany, Romania, Poland and Spain)
[65] Percentage based on sample countries (France, Germany, Romania, Poland and Spain)
[66] Eurostat: Second Interim Study Report N° 2019-0024 supporting the impact assessment
[67] Percentage based on sample countries (France, Germany, Romania, Poland and Spain) for ICT-SC)
[68] Percentage based on sample countries (France, Germany, Romania, Poland and Spain) for ICT-SC)

Table 26: Aggregated indicators for global market for products with digital elements in 2019 in the EU (SD & ICT-EXT-ADJ)[69]

[69] Eurostat: Second Interim Study Report N° 2019-0024 supporting the impact assessment.

2. Summary of (aggregated) costs and benefits - preferred policy option

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
Prevent internal market fragmentation	n/a	**Affected stakeholders:** • Economic operators, in particular hardware and software manufacturers • Public authorities (market surveillance authorities)
Enhanced security and transparency of products with digital elements	n/a	**Affected stakeholders:** • Users (B2B and B2C; public authorities)
Reduced number of cyber incidents	• By company/product: 20 to 33% of reduction of cybersecurity incidents • At aggregated level: approximately **EUR 180 to 290 billion annually for businesses** • No quantitative data for consumers and public authorities	**Affected stakeholders:** • Users (B2B and B2C; public authorities) • Economic operators, in particular hardware and software manufacturers (as regards reputational damage)
Improvement fundamental rights and in particular protection of personal data and privacy against breaches	n/a	**Affected stakeholders:** • Data subjects (citizens and consumers)
Increased turn-over due to conformity assessment		**Affected stakeholders:** • Notified bodies
Indirect benefits		
Decrease in risk mitigation costs (such as cyber insurance etc.)	n/a	**Affected stakeholders:** • Users (B2B and B2C; public authorities)
Higher uptake of digital solutions due to increased trust	n/a	**Affected stakeholders:** • Hardware and software manufacturers • Importers, distributors
Decrease in compliance costs, such as for operators of essential services under the NIS Directive and	• By company: o One off: 0.5 FTE (in average: EUR 33 280) for NIS entities	**Affected stakeholders:** • Business users • public authorities

entities subject to the GDPR	o Recurrent: 1-2% additional ICT security spending, for NIS entities (around 30 000 EUR by company, taking an average of 1.5%) • Aggregated: **EUR 6.95 bn**, with EUR 3.65 bn from one-off costs and EUR 3.3 bn recurrent costs.	
Increased global competitiveness by integrating security early in the development process and CE marking	n/a	**Affected stakeholders:** • Hardware and software manufacturers
Positive social impact, in particular reduced number of cybercrime	n/a	**Affected stakeholders:** • Businesses • Consumers • Public authorities • Citizens
Fewer incidents with a negative environmental impact	n/a	**Affected stakeholders:** • Society as a whole
Administrative cost savings related to the 'one in, one out' approach*		
Decrease in compliance costs, such as for operators of essential services under the NIS Directive and entities subject to the GDPR	• By company: o One off: 0.5 FTE (in average: EUR 33 280) for NIS entities o Recurrent: 1-2% additional ICT security spending, for NIS entities (around 30 000 EUR by company, taking an average of 1.5%) • Aggregated: **EUR 6.95 bn**, with EUR 3.65 bn from one-off costs and EUR 3.3 bn recurrent costs.	**Affected stakeholders:** • Business users • Public authorities
Prevent internal market fragmentation due to impending divergent national rules	n/a	**Affected stakeholders:** • Manufacturers of hardware and software

Table 27: Overview of Benefits (total for all provisions) – Preferred Option

*(1) Estimates are gross values relative to the baseline for the preferred option as a whole (i.e. the impact of individual actions/obligations of the preferred option are aggregated together); (2) Please indicate which stakeholder group is the main recipient of the benefit in the comment section;(3) For reductions in regulatory costs, please describe details as to how the saving arises (e.g. reductions in adjustment costs, administrative costs, regulatory charges, enforcement costs, etc.;); (4) Cost savings related to the 'one in, one out' approach are detailed in Tool #58 and #59 of the 'better regulation' toolbox. * if relevant*

II. Overview of (aggregated) costs – Preferred option							
		Citizens/Consumers		**Businesses**		**Administrations**	
		One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
	Direct adjustment costs *(triggered by security requirements, information obligations)*	N.A.	N.A.	*Familiarisation with new requirements: N.A. *Information on security of products with digital elements: N.A. *Secure product development: • By company/product: + 30.5% secure product development costs (with BaU costs at 50%) • Aggregated: **EUR 13.13 billion** (together with life cycle approach, taking into account BaU costs of 50%) ***** Testing costs • self-assessment: in average 18 400 EUR by product • Aggregated cost: **EUR 7 bn** *Standardisation costs: N.A.		* Familiarisation with new requirements: N.A. * Appointing new market surveillance authorities (*if applicable*): EUR 1 600 000 per year * ENISA (EU Agency for Cybersecurity) : For handling reporting of vulnerabilities and incidents: 4.5 FTE	
	Direct administrative costs	N.A.	N.A.	*Conformity assessment (third party-assessment): • By company/product: o third-party assessment: in average EUR 25 000 • Aggregated: **EUR 1.1 billion** *Documentation and reporting (including creating and updating DoC and technical documentation, affixing CE marking,and reporting): • By product/company: +9% product development costs • Aggregated: **EUR 7.8**		N.A.	N.A.

				billion (based on average product unit of EUR 140 000) * Accreditation framework: N.A. (for notified bodies)			
	Direct regulatory fees and charges	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
	Direct enforcement costs	N.A.	N.A.	N.A.	N.A.	*Monitoring and enforcement new requirements: • Additional enforcement costs by product: in average EUR 12 500 • Aggregated **EUR 7.7 billion**	
	Indirect costs	* Higher initial prices of products with digital elements with digital elements		* Higher initial prices of products with digital elements		N.A.	N.A.
Costs related to the 'one in, one out' approach							
Total	Direct adjustment costs	N.A.	N.A.	*Familiarisation with new requirements: N.A. *Information on security of products with digital elements: N.A. *Secure product development: EUR **13.13 billion** * Testing costs (self-assessment): • self-assessment: in average 18 400 EUR by product • Aggregated: **EUR 7 billion**			
	Indirect adjustment costs	N.A.	N.A.	N.A.	N.A.		
	Administrative costs (for offsetting)	N.A.	N.A.	*Certification: • By company/product: in average 25 000 EUR (BaU costs of 40% for hardware and 25% for software)			

				• Aggregated: EUR **1.1 billion** *Documentation and reporting: • By product/company: additional 9% of product development costs • **Aggregated: EUR 7.8 billion** (based on average product unit of EUR 140 000)		

Table 28: Overview of costs – Preferred option

ANNEX 4: ANALYTICAL METHODS

1. General approach

The appraisal of impacts by policy option relies on primary and secondary data collection. The collection of primary data included more specifically a workshop organised on 10 May 2022 by the contractors, an online targeted survey conducted by ICF SA, as well as a set of telephone interviews, including with SMEs. Furthermore, in the public consultation, respondents were asked questions about impacts on costs, competition and fundamental rights that are relevant for the impact assessment.

The online survey was launched on 16 May 2022 and at the moment of writing the impact assessment, the number of valid responses reached 24. In addition, the study team has conducted complementary interviews focused on cost estimates. Some additional consultations (with SMEs in particular) have been held as well.

Survey participants, workshop participants and interviewees have unanimously and consistently stressed the difficulties in providing exact figures. The main reason is that some of the requirements can be interpreted in different degrees of stringency which would impact costs in a very different way. Furthermore, the costs vary greatly depending on the type of product.

Quantitative cost estimations, even if gathered by the external Study, could not be triangulated and verified, and therefore have only been used for the cost aggregation to a very limited extent.

2. Key assumptions for the quantification of economic impacts

Several assumptions were made in order to quantify and compare the economic impacts of the different policy options.

Number of products on the market

In order to quantify the economic impacts of the policy options, the assumption was taken that **one company produces one product** as there is no possibility to know the number of products on the market. While this is an underestimation of the number of products, it is partially compensated by the fact that the number of companies is overestimated by using the ICT-EXT-ADJ indicator. 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.

Cybersecurity is mostly adding costs on the design of a produt, therefore looking at the number of products (e.g. number of connected devices) on the market, where some data is available, would not have been relevant. It would have been relevant to know more precisely how many products are developed by the manufacturers of hardware and software products on the EU market. However, no such data exists.

While a methodological choice had to be made in the IA report, other possibilities to estimate the number of products are not excluded, such as looking at the basic analysis of a typical company structure – possibly by category of size and scopes. It could have been estimated how many products a company would develop according to its size, which would have lead to similar number of produts (when combined with a more conservative indicator). Given that more than 99% of the market are SMEs, with 94% being micro

companies, most companies on the market would effectively not develop more than one or few products.

Alternative approaches for calculating the number of products have been considered for comparison, for instance such as dividing the turnover by the average cost of one unit of product with digital elements (EUR 140 000). This would however have led to an overestimation, as turnover also includes revenues. An alternative proxy could have been to take the investments in software/hardware to be divided by the average costs for one unit of product with digital elements (EUR 140 000)[70], but such data was not available.

Share of manufacturers already applying security requirements and testing

Furthermore, for quantifying the costs and benefits, it had to be assumed **how many manufacturers** would likely apply the full costs of secure product development, i.e. the percentage of companies that do not yet implement adequate security practices. Based on available data, it was estimated that currently **less than 50 %** of manufacturers have a systematic approach to product development in place.

This estimate was based on a number of assumptions and proxies, making most use of the scarce research and data available. More specifically: (i) according to a probe into a large number of products with digital elements developed by Microsoft, the introduction of secure development life cycles was found to reduce the number of vulnerabilities in a product by 66 %[71]; and (ii) based on the analysis of three different studies on the maturity of manufacturers of products with digital elements in the US (2010), Norway (2015) and Finland (2021), it was estimated that currently less than 50 % of manufacturers have a systematic approach to product development (see alos *Section 6.5)*.[72] While the study on US manufacturers is indeed less recent than the other two, there is evidence that shows that the overall picture has not changed since then: A very 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."[73], which suggests that there has been little (if any) improvement in how manufacturers approach product security. Therefore, it has been assumed that around 50% of manufacturers have currently adequate security practices in place for products with digital elements.

Cost estimations of secure product development

In order to aggregate the costs for integrating security in product development, a number of assumptions had to be made.

First, a percentage of additional product development costs had to be defined. The Venson model calibration[74] shows that the application of software security practices can impact the cost estimations ranging from a 19 % additional effort, on the first level of the security scale, to a 102 % additional effort, on the highest level of the scale. In order to

[70] This approach was used in the *Impact Assessment for the AI Act.*
[71] Fonseca and Vieira (2013): "A Survey on Secure Software Development Lifecycles", Software Development Techniques for Constructive Information Systems Design, p. 12.
[72] Microsoft's Security Development Lifecycle or the Comprehensive, Lightweight Application Security Process (CLASP): Geer, D. (2010), p. 12-16; 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; Kalle Rindell et al (2021): "Security in agile software development: A practitioner survey", Information and Software Technology Volume 131, March 2021, 106488.
[73] 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.
[74] 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.

classify the practices of secure software development, three broad categories were identified: (1) Security Requirements, and Design, (2) Secure Coding and Security Tools, and (3) Security Verification, describing different security practices according to five security levels (Nominal; High; Very High; Extra High; Ultra High)[75]. It is estimated that the baseline security requirements aimed for in policy option 3 and 4 would equal to the security levels between "high" and "very high". Implementing security product and process requirements would represent additional product development costs **between 19 % and 42 %[76], hence an average of 30.5 %.**

Second, an average estimation had to be made for the **cost of a developing a product with digital elements**. According to the data available, hardware product development costs are estimated between USD 50 000 and USD 300 000,[77] and software product development are similarly estimated around the same range (USD 50 000 and USD 250 000).[78] Taking the median value, the average price/cost of the development of a product with digital elements could be estimated at USD 150 000, i.e. approximately **EUR 140 000**. This average development costs is comparable to other estimations, such as the one done for the unit cost of an AI system in the context of the Impact Assessment for the AI Act.[79] By using the coefficient proposed by Venson (taking the average of 30.5 %), the additional costs of security requirements for a product with digital elements could represent on average EUR 42 700 for one product with digital elements unit if this product has no security features in place.

[75] Elaine Venson (2021) [See "Table 4.4 Practices", page 106]
[76] According to the coefficient evidenced by the researcher (SECU), [See "Table 5.13" on page 150].
[77] https://orbit-kb.mit.edu/hc/en-us/articles/205586653-How-much-would-it-cost-to-develop-a-hardware-product-
[78] https://www.uptech.team/blog/software-development-costs#:~:text=Ultimately%2C%20it%20comes%20down%20to,than%20700%20hours%20to%20develop
[79] See SWD(2021) 84 final, IA accompanying the AI Act, one AI system unit is estimated to cost 170 000 EUR.

ANNEX 5: BACKGROUND INFORMATION ON THE PROBLEM DEFINITION

1. Piecemeal coverage of cybersecurity in EU policies and impending national intervention

While EU law lays down cybersecurity requirements for some categories of products with digital elements, the vast majority of hardware and software products is currently not covered by any EU legal act. Nonetheless, under the NLF, the EU's blueprint for product regulation, there is a small number of legal acts providing for product-related cybersecurity requirements. These include the (RED)[80] together with a recently adopted delegated regulation,[81] which cover IoT devices outfitted with a radio interface; the Medical Devices Regulation (MDR)[82] as well as the In Vitro Diagnostic Medical Devices Regulation,[83] which cover both tangible medical products as well as software; the relevant regulations on motor vehicles and their trailers, which also provide, among others, for empowerments the adoption of implementing or delegated acts concerning uniform procedures and technical specifications or updating technical requirements that may also concern cybersecurity-related aspects;[84]the Measuring Instruments Directive (MID),[85] which regulates measuring instruments or the Commission's recent proposals for a Machinery Regulation (MR),[86] as well as a Regulation laying down harmonised rules on AI.[87]

In addition, there are a few European product laws that provide some rules regarding the cybersecurity of products, albeit only in a *partial* manner: These include the Toy Safety Directive,[88] which regulates the safety of toys; the Machinery Directive,[89] which covers machinery products, including software ensuring safety functions; the Non-Automatic Weighing Instruments Directive;[90] the ATEX Directive,[91] which covers equipment and protective systems intended for use in potentially explosive atmospheres and covers some software related risks. An example of this partial coverage is the Non-Automatic Weighing Instruments Directive, which requires manufacturers to ensure that instruments are not adversely affected by external equipment connected to them and that instruments have no characteristics likely to facilitate fraudulent use, but lacks a more comprehensive approach to cybersecurity.

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.

The exploratory study contracted by the Commission and conducted in 2020-2021 to assess the need for horizontal cybersecurity requirements for products with digital

[80] RED: Directive 2014/53/EU.
[81] RED Delegated Act: 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.
[82] MDR: Regulation (EU) 2017/745.
[83] MDR: Regulation (EU) 2017/746.
[84] Regulation (EU) 2018/858 and Regulation (EU) 2019/2144
[85] Directive 2014/32/EU.
[86] Machinery Regulation (Proposal): COM(2021) 202 final.
[87] AI Act (Proposal): COM(2021) 206 final.
[88] Toy Safety Directive: 2009/48/EU.
[89] Machinery Directive: 2006/42/EU.
[90] Weighing Instruments Directive: 2014/31/EU.
[91] ATEX Directive 2014/34/EU.

elements conducted a **gap analysis**,[92] comparing the cybersecurity objectives of certification schemes set out in the Cybersecurity Act (Article 51)[93] against the identified cybersecurity-relevant requirements of **37 pieces of EU legislation** concerning ICT products, including all legislation related to the NLF, as well as legislation with a strong link with cybersecurity and data protection, which can affect even indirectly and to a limited extent manufacturers (e.g. the eIDAS Regulation, GDPR,[94] the NIS Directive, Radio Equipment Directive, General Product Safety Directive (GPSD)).[95]

Among the study's **most relevant findings of the gap analysis** the following could be mentioned:

- The **current EU legislative framework does not cover all security objectives** of the Cybersecurity Act, with **fragmentation and gaps** related to cybersecurity requirements for products with digital elements. This is illustrated below.

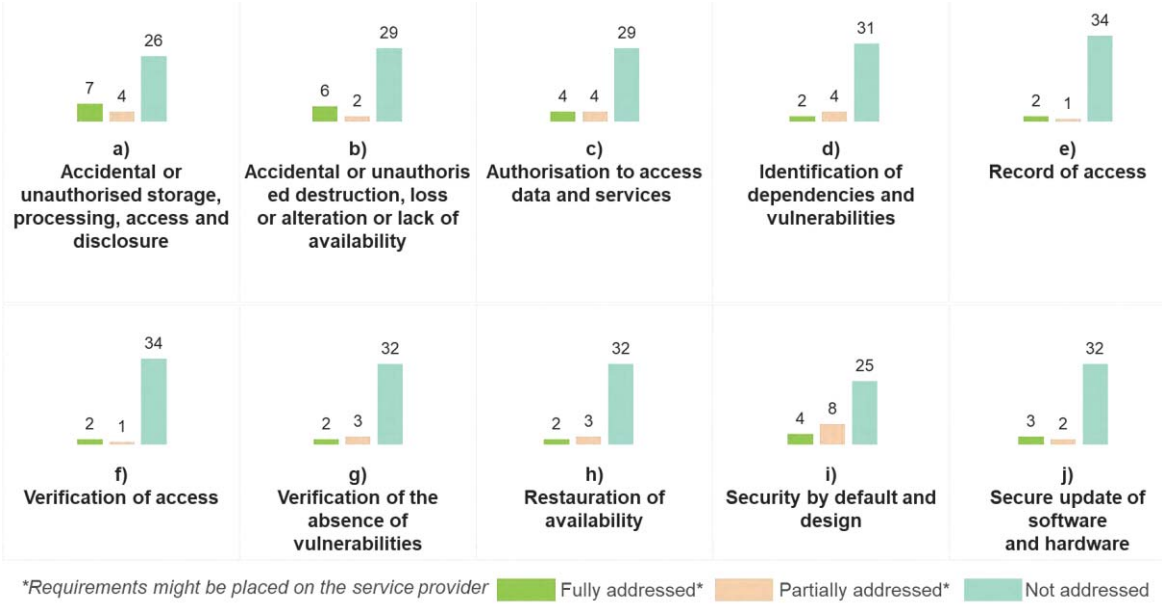


Figure 11: Gap analysis of the current EU legislative framework

- The legislation related to the **NLF does not address fully the cybersecurity requirements** for products with digital elements;
- Some pieces of legislation contain cybersecurity requirements that concern services rather than products and are therefore addressed to entities/service operators. While they can **indirectly affect the cybersecurity level of products with digital elements** used to operate the service, **they are not setting any clear obligations on the manufacturers of products with digital elements.** In such cases (for example GDPR obligations on data controllers or NIS obligations on

[92] Section 2.2 of the final report of the *Study on the need of Cybersecurity requirements for ICT products*, pages 52-61.
[93] To date, the Cybersecurity Act provides the most comprehensive set of cybersecurity requirements in EU law.
[94] The GDPR does not impose obligations to manufacturers of products but only to controllers processing personal data, yet the Regulation encourages them to respect the principle of data protection by design and by default when they develop new products.
[95] 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.

operators of essential services), the way the service operators implement the respective requirements (where there is some room for discretion) may affect in various ways the manufacturers of products with digital elements. This, in the absence of corresponding legislation setting requirements for security of products, may ultimately lead to misalignments of cybersecurity requirements and additional complexity for the manufacturers;

- There are **different levels of granularity in the definition of the scope** of products covered by the EU legislative framework that may lead to uneven burden on manufacturers of similar products or of products that may have similar importance from a cybersecurity point of view;
- There are **different levels of granularity** of **cybersecurity requirements** in the legislation in scope;
- Some pieces of legislation require the manufacturer or service provider to issue **"notifications" in case of a security breach or risk**,[96] which is an objective that is not present in the Cybersecurity Act, while for some other relevant pieces of legislation such notification obligation does not exist. Such notifications may ultimately have consequences on the cybersecurity of the products that may have been concerned by such incidents and, absent a horizontal approach on similar products, may lead to an uneven playing field for manufacturers and/or uneven protection of security; and
- The **safety aspects** of products in scope are overall **more addressed than the security aspect**s.[97]

Furthermore, the follow-up study[98] to support this impact assessment, contracted by the Commission in 2022, found in its preliminary in-depth analysis of relevant existing EU legislation, notably product-related, that requirements regarding software are very rarely covered by such legislation, and, even when this is the case, it is difficult to ascertain the precise cybersecurity requirements or obligations. Furthermore, it found that most of the pieces of legislation targeting product safety do not address the cybersecurity of the products falling under their scope. Moreover, the follow up study also analysed the interplay between the regulatory intervention and the Commission Data Act[99] proposal and concluded that the scope of the latter is different and hence the two pieces of legislation would be complementary.

See the more detailed preliminary analysis conducted by the study in Annex 8

2. Additional drivers not addressed by this intervention

In addition to the main drivers described in the problem definition, the Commission has identified 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

[96] For example, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector provides that: *"In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.". Also,* legislation connected to the NLF mandates the need to contact authorities in case a risk is identified on a product.

[97] Safety refers to the prevention of physical harm as a result of accidents, while security refers to the prevention of crime.

[98] Study supporting the Commission preparatory work for the Cyber Resilience Act – N° 2019-0024.

[99] Data Act Proposal: COM(2022) 68 final.

products. These are described only very briefly in the impact assessment itself, as the regulatory intervention would not address them.

Lack of bargaining power of users

As described above, products with digital elements markets are often characterised by the presence of a few large manufacturers as a result of *economies of scale* and *vendor lock-in*. For example, economies of scale play a significant role when it comes to producing semiconductors, as the manufacturing process is characterised by major fixed costs.[100] [101] While the development of large-scale software solutions, such as operating systems, also comes at a high cost, concentration in software markets is rather explained by vendor lock-in and high switching costs: As computer programmes are usually developed in such a way that they are compatible with a specific operating system, users cannot simply switch to another operating system when they are not satisfied with the security properties of the system that they have been using so far. For example, when it comes to Microsoft's operating system Windows, this has led the Commission to conclude that the company *"can behave independently of its end-customers"*.[102]

Irrespective of the reasons why some hardware and software products markets are controlled by a relatively small number of manufacturers, there are clear implications for the cybersecurity of the products offered on these markets and the security needs of users: businesses, such as operators of essential services under the NIS Directive, often lack the negotiating power to ensure that hardware and software suppliers provide products matching their own security needs.[103] [104] This is even more so the case when it comes to individual consumers.[105]

Lack of qualified security professionals

While products with digital elements markets do not provide the right incentives for hardware and software manufacturers to take cybersecurity seriously, manufacturers are also constrained by a shortage of information security professionals in the labour market. In a recent report, the European cybersecurity agency ENISA concludes that "there is a lack of skilled and qualified personnel in the labour market to work in cybersecurity roles and who can sufficiently address the range of cyber threats posed".[106] The International Information System Security Certification Consortium reports that in 2021 the gap in cybersecurity professionals in Europe amounted to 199 000 (up from 168 000 in 2020). In North America, where much of the hardware and software used in Europe is designed or developed, the skills gap amounted to 402 000 (up from 376 000 in 2020).[107] According to another recent survey, 55 % of businesses worldwide report unfilled information security vacancies, with 60 % of businesses reporting that it takes three months or longer to fill a vacancy.[108]

---

[100] Kenneth Flamm (2018): "Measuring Moore's Law: Evidence from Price, Cost, and Quality Indexes", Working Paper 24553, *NBER working paper series*.
[101] Statement by Executive Vice-President Margrethe Vestager on the Commission decision to accept commitments by Broadcom to ensure competition in chipset markets for modems and set-top boxes, 7 October 2020.
[102] Case COMP/C-3/37.792 Microsoft, p. 126.
[103] Tania Wallis (2020): "Achieving cybersecurity improvements through Enterprise Systems Engineering", *ASEC 2020 Proceedings*, p. 2.
[104] https://www.computerweekly.com/news/450415989/How-IT-can-be-more-defensible.
[105] Dutch Safety Board (2021), p. 89.
[106] ENISA (2021): "Addressing the skills shortage and gap through higher education", p. 5.
[107] (ISC)² (2021): "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021", p. 25.
[108] ISACA (2021): "State of Cybersecurity 2021. Part 1: Global Update on Workforce Efforts, Resources and Budgets", p. 8.

While a European initiative on security of products with digital elements cannot address deficiencies in the labour market, it is worth noting that the European Union has launched a number of initiatives to reduce the digital skills gap in general and the cybersecurity skills gap in particular. For instance, the Digital Europe Programme supports the development of a skilled talent pool of digital experts with EUR 580 million over the period 2021-2027, explicitly mentioning skills related to cybersecurity as one of its operational objectives. In addition, the European Cybersecurity Skills Framework developed by ENISA aims at creating a common understanding of the roles, competencies and skills required across the EU to alleviate the skills shortage in information security.[109]

Lack of cybersecurity awareness and skills of users

Users often choose products with digital elements ill-suited for their needs or configure them in such a way that they can be breached easily because they are either not fully aware of the risks associated with the products they deploy or lack the necessary technical skills. According to a recent survey amongst 3 000 consumers, while 69 % consider themselves as being good or very good in protecting their accounts, two thirds reuse passwords either for some or sometimes even for all their accounts. In addition, only one third are able to correctly define a set of basic internet security terms.[110] A study from June this year has surveyed 553 parents in the UK "that families do not consider home IoT devices to be significantly different in terms of threats than more traditional home computers, and believe the major risks to be largely mitigated through consumer protection regulation. As a result, parents focus on teaching being careful with devices to prolong device life use, exposing their families to additional security risks and modeling incorrect security behaviors to their children."[111] The lack of awareness not only applies to consumers but also to business users. For example, only half of company leaders and a third of employees acknowledge the risk that cybercrime poses to their organisations.[112]

Update habits are one way to measure the awareness of users of the risks associated with the technology that they use. For instance, Android users are known to delay or even entirely forgo updating applications installed on their systems despite the fact that updates are essential to patching critical holes in users' mobile devices.[113] It does not come as a surprise that generally speaking inexperienced users are much less likely to install crucial security updates than proficient IT users.[114] Similarly, companies regularly fail to patch critical holes in their networks, with a large number of incidents being the result of unpatched but long known vulnerabilities in products.[115] When it comes to cybersecurity skills, even companies regularly fail to configure their systems correctly. For example, cybersecurity incidents following a misconfiguration of cloud systems were responsible for the exposure of more than 33 billion data records in 2018 and 2019.

[109] For more details, see https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.
[110] Google/Harris Poll (2019) https://services.google.com/fh/files/blogs/google_security_infographic.pdf.
[111] Sarah Turner, Nandita Pattnaik, Jason R.C. Nurse, Shujun Li (2022): '"You Just Assume It Is In There, I Guess": UK Families' Application And Knowledge Of Smart Home Cyber Security'.
[112] Grayson Kemper (2019): "Improving employees' cyber security awareness", *Computer Fraud & Security, Volume 2019*, Issue 8, August 2019, Pages 11-14.
[113] M. Oltrogge, Y. Acar, S. Dechand, M. Smith, and S. Fahl: "To Pin or Not to Pin—Helping App Developers Bullet Proof Their TLS Connections" in Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC'15. Berkeley, CA, USA: USENIX Association, 2015, p. 240.
[114] Mathur, Malkin et al. (2018): "Quantifying Users' Beliefs about Software Updates", p. 1.
[115] Check Point (2021): "Cyber Security Report", p. 55.

Organisations mostly affected were tech companies, health care providers and governments.[116]

The EU is addressing digital skills through the Digital Europe Programme, which supports the development of a skilled talent pool of digital experts with EUR 580 million over the period 2021-2027, explicitly mentioning skills related to cybersecurity as one of its operational objectives. In addition, ENISA together with the Commission and the Member States organises European Cyber Security Month on an annual basis to promote cybersecurity among EU citizens and organisations and provide up-to-date online security information through awareness raising activities and sharing of good practices.

While awareness and lack of skills are important sources of incidents, manufacturers often do too little ensure that their products can be used securely "out of the box" by inexperienced users. One way to help inexperienced users is to ship products with all security settings set to maximum (*security by default*) or by automatically applying security updates without requiring an intervention by the user.

Asked in the public consultation to which extent consumers understand the cybersecurity properties they should expect from products and to which extent they have the skills to operate them securely, consumers organisations gave a rating of only 1.67 (on a scale from 1 to 5).

[116] DivvyCloud (2020): "2020 Cloud Misconfigurations Report. Breaches Caused by Cloud Misconfigurations Cost Enterprises Nearly $5 Trillion in 2018 and 2019", p. 4 and 10.

ANNEX 6: GLOBAL DEVELOPMENTS

1. United States

In May 2021, an Executive Order (EO)[117] was issued by the US President, charging operational federal agencies, including the National Institute of Standards and Technology (NIST) in the US Department of Commerce, with developing guidelines for enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.[118]

The EO established a detailed plan for taking steps to secure the federal software supply chain and called for NIST to publish guidelines for establishing best practices to detect vulnerabilities and requirements that all critical software delivered to government customers, including a software bill of materials to ensure transparency of supply chain. It also included milestones that agencies must meet to demonstrate progress toward the goals. In 2021, NIST also initiated a pilot program on cybersecurity labelling for IoT products. In the same year, as required by the EO, NIST released its definition of critical software and published guidance for outlining security measures for critical software use and minimum standards for manufacturers' testing of their software source code. In mid-2021, the National Telecommunications and Information Administration (NTIA) released a minimum definition of a software bill of materials (SBOM). In February 2022, NIST issued guidance for supply chain security.[119]

In July 2021, both the House of Representatives and the Senate of United States of America began drafting legislation in two separate committees. In particular, the House's Homeland Security Committee introduced seven bipartisan bills, five of which focused strictly on strengthening cybersecurity, while the Senate's Homeland Security and Governmental Affairs Committee introduced 'The Supply Chain Security Training Act,' calling it a *'bipartisan legislation to help protect against cybersecurity threats and other technological supply chain security vulnerabilities that arise when the federal government purchases services, equipment or products.'*[120]

Recently, the US Department of Defense released a report titled 'Securing Defense Critical Supply Chains',[121] where it presents its priorities and capabilities to make stronger the USA industrial base and to create a network of domestic and applied supply chains to meet national security needs. In particular, the report identifies cyber posture, characterised by industrial security, counterintelligence and cybersecurity - as one of the strategic enablers necessary to build overall supply chain resilience.[122]

---

[117] (EO) 14028 on Improving the Nation's Cybersecurity:

[118] The EO stated that: *'Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).*'

[119] Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e.

[120] https://www.hsgac.senate.gov/media/majority-media/after-passing-house-peters-and-johnson-legislation-to-help-secure-federal-information-technology-supply-chains-against-security-threats-heads-to-president-to-be-signed-into-law.

[121] https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

[122] See Hogan Lovells (2022), The department of Defense's report on Securing Defense-Critical Supply Chains" April 12

2. United Kingdom

Some developments in terms of supply chain security have been furthered also in the United Kingdom. In May 2021, the U.K. government announced that it was seeking advice on defending against digital supply chain attacks from organisations that either consume IT services, or Managed Service Providers that provide software and services. While the feedback has not been released to the public yet, the U.K. government has noted that it will result in the re-evaluation of supply chain risks, reviewing policies, and likely implementing new guidelines and frameworks to strengthen specific areas of digital supply chain security. It could also mean the introduction of new, country-wide legislation for software firms and IT service providers. Moreover, following a work carried out in 2018 on telecom supply chain security, in May 2022, the Department for Digital, Culture, Media, and Sport (DCMS) opened up a survey that closed in early July and invited comments from industry experts and technology organisations on stepping up supply chain security across the UK.

3. Asia: examples of Japan and Singapore

The Ministry of Economy, Trade and Industry of Japan (METI) envisages the development of a super-smart society in which cyberspace and physical space are integrated in a sophisticated manner, the so-called "Society 5.0". To meet the cybersecurity challenges stemming from this scenario, the Japanese government published the Cyber-Physical Security Framework (CPSF) Ver1.0 on April 18, 2019, which outlines security measures against new risks in Society 5.0 and propose a "Three-Layer Approach" to articulate risks and appropriate measures in the whole supply chain.[123] The second layer is represented by the actual connection of the physical and cyberspace, namely the IoT systems themselves. In this context, the METI published in March 2020 a draft of the "IoT Security Safety Framework" with a guideline on how to guarantee security for IoT devices and systems. In this context, METI introduced a method for classifying IoT devices and systems based on their risk profiles. IoT devices are classified alongside two axes: (1) the degree of difficulty of recovery from the incidents; (2) perspective of economic impact from the incident.

The Cybersecurity Labelling Scheme (CLS) is an instrument issued by the Cyber Security Agency of Singapore to manage the cybersecurity of consumer IoT products. The Cybersecurity Labelling Scheme is a voluntary scheme, except for Wi-Fi Routers, for which it is mandatory to meet the baseline cybersecurity requirements. The CLS covers Wi-Fi Routers and Smart Home Hubs, and it is open to all other categories of IoT devices. The labelling scheme foresees different level similar to the assurance levels in EU certification schemes. The highest level involved third-party testing.

[123] See METI (2019), Cyber/Physical Security Framework (CPSF) Formulated. Available here.

ANNEX 7: COMPARISON OF THE RED DELEGATED REGULATION VS POLICY OPTION 4 (COMPREHENSIVE HORIZONTAL REGULATION FOR ALL PRODUCTS WITH DIGITAL ELEMENTS)

	Horizontal cybersecurity requirements for all products with digital elements *(including inter-connected radio-equipment)*	**RED Delegated Regulation (RED DA)**
Scope		
internet-connected radio equipment and wearable radio equipment ('wireless'), including laptops, smartphones and tablets	yes	yes
Wired-only connected products	yes	no
Non-embedded (standalone) software	yes	no
Non-radio components (e.g. processors)	yes	no
Requirements & obligations		
Cybersecurity dimension (protection of network, ensure data protection and relevant aspects on privacy and fraud dimension	yes (more specific – e.g. addressing cybersecurity risks to availability, integrity, confidentiality; vulnerability handling, transparency and information to users' obligations, etc.; the more specific requirements would fit into the very generic cybersecurity requirements of RED Delegated Regulation)	yes (very generic)
Duty of care and whole life cycle	yes	no
Conformity assessment		
Conformity assessment	Self-assessment, and third-party assessment for a narrow share of critical products, and potentially mandatory EU certification for highly critical products	Self-assessment

Table 28: Comparison RED Delegated Regulation vs Policy option 4

ANNEX 8: EXTRACT FROM THE PRELIMINARY FINDINGS OF THE STUDY SUPPORTING THE COMMISSION PREPARATORY WORK FOR THE CYBER RESILIENCE ACT (N° 2019-0024)

- **A focus on software**

The analysis revealed that software is rarely explicitly mentioned in the legislative texts of relevant legislative acts, and even when this is the case, it might be difficult to ascertain the relative cybersecurity requirements or obligations. This is particularly true for pieces of legislation that are currently under review, such as the Machinery Directive - which makes limited references to hardware and software when talking about control systems (Essential Health and Safety Requirement 1.2) - and the GPSD - which does not currently provide enough legal certainty about the coverage of the specific features of new technology products, such as software updates or the evolving nature of new technologies.

The EC aimed to update these pieces of legislation to address challenges brought by new technological developments,[124] hence clarifying the role of software with regard to the overall product functioning and its possible impact on health and safety of consumers. To do so, the **Proposal for a Regulation on Machinery Products** further clarifies the definition of 'safety component' to include not only physical components but also non-physical components such as software performing a safety function and placed independently on the market (Article 3(3)). Furthermore, it adapts the definition of 'machinery', including machinery missing only the upload of a software intended for the specific application of the machinery under it and not under the definition of partly completed machinery (Article 3(1f)). However, it must be noted that pursuant to Article 2(2m) it would not apply to electrical and electronic products falling within the scope of application of Directive 2014/35/EU or Directive 2014/53/EU, such as household appliances, audio/video equipment and information technology equipment.[125] The **Proposal for a Regulation on General Product Safety (GPSR)** updates the definition of 'product' included in Article 3(1) to *'items that are interconnected or not to other items'*, and it expands the criteria for assessing the safety of products (Article 7h) to include the appropriate cybersecurity features necessary to protect the product against external influence. It is also worth mentioning that the GPSR will take over the role of 'safety net' (as the GPSD before) with regard to non-harmonised consumer products and to the harmonised consumer products for the aspects that are not covered by harmonised legislation.[126]

Software is also mentioned in the **AI Act** when defining AI systems (Article 3). The proposal directly links AI systems to software by clarifying that this software possesses key functional characteristics (listed in Annex I) and aims to accomplish a set of human-defined objectives.

The reference to software is more explicit in other pieces of existing EU product safety legislation. This is the case for: the **RED**, which covers software "*allowing radio*

[124] In this regard, it is possible to refer to: (i)Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council. P.3; and (ii) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products. P.1

[125] This input was shared by Mark D. Cole, Professor for Media and Telecommunication Law at the University of Luxembourg, member of the Advisory Board.

[126] This input was shared by Mark D. Cole, Professor for Media and Telecommunication Law at the University of Luxembourg, member of the Advisory Board.

equipment to be used as intended" (Article 4); the **MDR**, which already reflects the ongoing digitalisation process and covers software (Article 2), while addressing the cybersecurity of both hardware and software; and the **Measuring Instrument Directive** (MID) which mentions software within the requirements placed on the products falling under its scope and defines specific conformity assessment modules for electronic systems or systems containing software (see Annex I, II, VIII and IX).

Furthermore, other pieces of EU legislation refer to software in their provisions. For instance, the **Consumer Sales Directive** (CSD) includes in its scope the notion of goods with digital elements, and thus applies to any digital content or digital service. Recital 14 of the CSD clarifies that digital content incorporated in or inter-connected with a product under the scope *"can be any data which are produced and supplied in digital form, such as operating systems, applications and any other software*" regardless of the time of installation (before or after the sale). Software is also used to define compatibility and interoperability aspects of the goods falling under the CSD (Article 2). Another example of reference to software is the **Market Surveillance Services Directive** (MSD) which mandates manufacturers (Article 15) to provide, upon request of the approval authorities, information about software and algorithm which are necessary to demonstrate the conformity of a vehicle, system, component or separate technical unit. Software is also included in the notion of a product (Article 3) provided by the **eIDAS regulation** which defines product as "*hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services".*

In conclusion, the new challenges brought by new technological developments prompted the EC to update some pieces of legislation, by clarifying the role of software within their provisions (e.g., MR, GPSR, AI Act) in light of their relevance for security of networks and rights of individuals in an increasingly connected environment. Software is considered by several pieces of EU legislation either as a way to define the products falling under their scope (e.g., MDR, RED, CSD, eIDAS) or to highlight certain characteristics of products which deserve particular attention from their manufacturers (e.g., MID, MSD).

- **Approach to safety and security in the EU legislative framework on products**

The exploratory study concluded that the EU legislation on products focuses mainly on safety rather than security (see finding #7). This finding appears to be consistent with the intent of the EC to align the EU regulatory framework on products with the reference provisions set by Decision 768/2008/EC[127](part of the NLF) which placed obligations on economic operators along the supply chain (e.g., manufacturers, importers, distributors) to ensure the health and safety of consumers.[128] However, the NLF does not contain provisions mandating economic operators to account for cybersecurity during the risk assessment and subsequent identification of NLF certification modules and self-declaration. As a result, security is accounted for only in some pieces of legislation which do not set horizontal cybersecurity requirements.

Most of the pieces of legislation targeting product safety do not address the cybersecurity of products falling under their scope. For instance, the **Recreational Craft and Personal Watercraft Directive** (RRD) does not place any cybersecurity requirements on the products falling under the scope of the analysis nor on the main economic operators considered in Chapter II of the Directive. The essential requirements laid down in Annex

[127] Information available at: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_fr

[128] For instance, Annex I - Reference provisions for community harmonisation legislation for products, Article R2 (4 and 7), Article R4 (4 and 6) and Article R5 (2).

I of the RRD mainly concern safety aspects such as the identification, the structure, the stability and other physical aspects of the products in scope. The **Pressure Equipment Directive** (PED) represents another example of a directive which covers safety without considering the security (and cybersecurity) aspect. The PED contains (Annex I) a set of general, design, manufacturing and other requirements that focus strictly on safety without safeguards aimed at addressing the cybersecurity of the measuring instruments.

Over the past years, the EC has been seeking to address the new challenges on consumer safety posed by new digital technologies (e.g., software, AI, IoT) by putting forward pieces of EU product legislation which clearly addressed cybersecurity when connected to consumer safety. When looking at sector-specific regulation, it is possible to refer to two examples, namely the Measuring Instruments Directive (MID)[129] and the MDR. Within Annex I, the **MID** includes essential requirements both on suitability of the equipment (ESHR 7), defining additional precautions to be used when the product is associated with a software and, on protection against corruption (ESHR 8). The requirement addresses the risk for a measuring instrument to be connected with another device and to be subject to an inadmissible influence. The **MDR** lays down essential requirements for medical devices that function through an electronic system or that are software themselves[130]. These requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures. It is important to point out that the MDR does not clarify which risks the regulation is seeking to address. Particularly, the MDR does not distinguish between functionality and safety risks as the poor functioning of a medical device has usually a direct (negative) effect on the health and safety of its user. It follows that the requirements set by the regulation focus on the reliable performance of the device[131]. The most relevant requirements accounting for the cybersecurity of the products falling under the scope of the MDR are No. 14 (Construction of devices and interaction with their environment) and No. 17 (Electronic programmable systems), both included in Annex I of the regulation. Additionally, considering more horizontal pieces of legislation, the **RED** took another step forward in addressing cyber-related risks of inter-connected devices and wearables, with the RED Delegated Act which shall apply form 1 August 2024. In fact, the Directive foresees two requirements in Article 3(d), (e) and (f) which aim to address network protection and incorporate safeguards into products so to protect users' privacy and personal data as well as to protect them against fraud.

More recently, the **GPSR** proposal addresses cybersecurity risks that have an impact on the safety of consumers by mandating products to possess cybersecurity features (Article 7h) that can protect them from external influences (e.g., hacking). However, it is worth pointing out that manufacturers are mandated to consider cybersecurity risk only if Article 6(1a) on harmonised European standards and Article 6(1b) on national requirements do not apply. Furthermore, the **Machinery Regulation proposal** (MR**)** mandates new requirements (Annex III – 1.1.9 and 1.2.1) on the protection of machinery against corruption and unauthorised access. Particularly, while introducing the concept of security by design for machinery and control systems (i.e., those connected should be designed in such a way to minimise their exposition to hazardous situations), the requirements also stress the importance in the identification and subsequent protection of software and data that impact on the compliance of the machinery with health and safety requirements.

[129] MID: Directive 2014/32/EU.
[130] https://ec.europa.eu/health/system/files/2022-01/md_cybersecurity_en.pdf, p. 4.
[131] Wendenhorst C. (2020). Safety and Liability Related Aspects of Software, p. 51.

On the other hand, when it comes to certain existing pieces of EU legislation discussion are ongoing on whether they should take into account cybersecurity aspects, such as the **Toy Safety Directive** (TSD). In this regard, the European Parliament expressed concerns in relation to the new risks posed by connected toys, particularly when they pose threat to child safety, security, privacy and mental health. Furthermore, while pointing out that connected toys show inadequate level of security, with no or limited measures to prevent cyber threats, the European Parliament called on the EC by updating the TSD or exploring other options to increase consumer protection such as the adoption of a horizontal piece of legislation on cybersecurity requirements for connected products and associated services[132]. However, it is important to note that the Delegated Regulation adopted under the RED in October 2021 partially addressed the need for cybersecurity requirements on wireless toys (Article 1(2)c).

In conclusion, while recognising the efforts put forward by the EC in relation to an increased **cybersecurity of products marketed within the EU, security, and more specifically cybersecurity, still does not appear to be broadly embedded in the EU legislation on product safety[133]**. The requirements currently in place target specific types of products (e.g., medical devices, measuring instruments) and/or are cross-sectoral but focus only on digital devices with certain characteristics (e.g., wireless).

- **Product life cycle approach**

The EU legislation on products currently relies on the concept of '*placing a product on the market'*. This notion appears to be challenged by new technological developments that allow products to evolve after this moment in time. For instance, software updates can change the functionalities of the product on which the software operates.

Discussions on whether the NLF could be updated to incorporate the concept of a product life cycle approach are currently ongoing. However, as highlighted by an expert supporting the study, stakeholders have suggested that the focus of the NLF should remain on setting common reference provisions for placing a product on the market, with changes post-market placement being better addressed on an *ad-hoc basis* by individual pieces of legislation. Another possibility raised by stakeholders is to accommodate these developments by amending the suite of conformity assessment modules of the NLF, for instance by introducing a new component related to post-market placement verification. All in all, while being currently under evaluation, the NLF is not yet subject of a proposal to update and modernise it (i.e. no impact assessment is currently planned).

As a notable exception to this static view of product compliance, the **MDR** foresees (in Annex I (3)) a specific requirement placed on manufacturers to establish, implement, document and maintain a risk management system for their products, meaning a process throughout the entire life cycle of a device, requiring regular systematic updating. Similarly, but more recently, the **AI Act** proposal requires high-risk AI systems to be subject to a risk management system (Article 9). Moreover, the proposal sets requirements on record-keeping (Article 12) and accuracy, robustness and cybersecurity which shall also take into consideration the life cycle of high-risk AI systems. Furthermore, the activation of the **delegated acts under the RED** addresses software updates.

[132] European Parliament (2021). Report on the implementation of Directive 2009/48/EC of the European Parliament and of the Council on the safety of toys (Toy Safety Directive).

[133] It is worth mentioning that, as highlighted by Mark D. Cole of the Advisory Board, in the Impact Assessment for the GPSR (SWD(2021) 168 final) it is stated that gaps in sectoral legislation (such as wired devices not covered by the RED delegated act) might be covered by the GPSR in its role of safety net.

Additionally, draft legislative proposals pertaining to the updating of EU harmonisation legislation, often take more of a product life cycle approach, reflecting the fact that change in products may occur post market placement, either due to software updates/upgrades or due to the circular economy. For instance, the **GPSD** is currently under revision to accommodate the ever-evolving nature of digital technologies (i.e., GPDR proposal). In fact, the Sub-group on AI, connected devices and other challenges for new technologies to the Consumer Safety Network recommended that the revision of the GPSD should clarify that products should be safe during their whole lifespan to accommodate for the new risks brought by digital technologies. Against this background, the **GPSR** put emphasis on the need for the product to be safe over its entire lifespan. In this regard, Article 12 (cases in which obligations of manufacturers apply to other economic operators) defines circumstances under which any economic operator that modifies *"a product in such a way that conformity with the requirements of this Regulation may be affected, should be considered to be the manufacturer and should assume the obligations of the manufacturer".*[134] The **MR** proposal also provides an example of how some aspects of changes (e.g., to software updates, AI and machine learning technologies) to products post-placement can already be addressed at the moment a product is placed on the market. The MR requires an upfront risk assessment as to any potential changes post-market if these risks bring a product into non-compliance with the essential requirements (Annex III -1c). Currently, there are significant challenges related to the issue of built-in obsolescence (i.e. products are designed to be replaced in a certain timeframe and will therefore no longer be supported). Within this context, there is a key question of 'for how long (per product type) economic operators should provide security updates.[135]

- **Responsibilities set along the value chain**

Since its adoption in 2008, the NLF represented an important step forward in the strengthening of the EU Single Market. The NLF identifies the economic operators having an impact on product safety, while also defining their respective responsibilities and obligations within the value chain. Consequently, the sectoral and product-focused NLF-aligned legislation followed this framework to guarantee legal certainty to consumers and businesses operating within the Single Market. Nevertheless, new technological development and the shift toward greener and circular economy brought a broader set of economic operators to play a relevant role within the value chain. The EC is conducting an evaluation, assessing whether the NLF continues to be fit for purpose in the current economic reality and changing digital environment.[136] [137]

The 2019 **Market Surveillance Regulation (MSR)**, which came into effect in 2022, introduced for most NLF-aligned laws (see Article 4(5)) the requirement for an EU-based economic operator in order to place a product on the market. One of the options is to contract an authorised representative (which was actually already defined in the NLF), while another is to use a fulfilment service provider (newly defined in the MSR).

[134] It is worth noting that the modification creates new obligations on other operators only when such modification is 'substantial'. The same article describes the criteria that should be met to consider modification as 'substantial', namely: (a) the modification changes the intended functions, type or performance of the product in a manner which was not foreseen in the initial risk assessment of the product; (b) the nature of the hazard has changed or the level of risk has increased because of the modification; and (c) the changes have not been made by the consumer for their own use.

[135] This input was shared by Mark Whittle Director of CSES Europe, member of the Advisory Board.

[136] See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12654-Industrial-products-evaluation-of-the-new-legislative-framework_en

[137] Information on the supporting study is available at: https://op.europa.eu/en/publication-detail/-/publication/f26b695f-cce7-11ec-a95f-01aa75ed71a1/language-en

However, manufacturers/importers are not mandated to use an authorised representative or fulfilment service provider.[138] This regulation represented a first step to address the challenges faced by market surveillance authorities when tracing non-compliant products imported into the Union and identifying the responsible entity within their jurisdiction.

The **MDR** represents a comprehensive piece of legislation covering all economic operators in the value chain such as manufacturers[139] (Chapter II, III and V), importers (Article 13), authorised representatives (Article 11) and distributors (Article 14). It is worth noting that manufacturers encompass also software manufacturers as long as their products have a medical purpose and thus can be classified as a medical software. While mainly targeting the manufacturers of medical devices, the MDR sets obligations on several economic operators to make sure that there are always multiple stakeholders responsible for provisions set by the regulation, particularly when products are manufactured from non-EU countries. Similarly, the RED stresses that all economic operators intervening in the supply and distribution chain should take appropriate measures to ensure that they only make available on the market radio equipment which is in conformity with the Directive and therefore it is necessary to provide for a clear and proportionate distribution of obligations (recital 27).

On the other hand, responsibilities along the value chain had to be further clarified within the proposals for some pieces of legislation currently under review, as in the case of the **GPSR** (recital 24) and the **MR** (recital 25). It is interesting to note that the latter also clarifies that when a machinery is substantially modified according to the definition, the one that modifies the machinery becomes manufacturer and must comply with the relevant obligations (recital 36 and Article 15). Furthermore, as the complexity of the machinery supply chain is increasing, there is a general obligation of cooperation of third parties involved in the machinery supply chain, other than economic operators.

It is also worth noting that the **NIS2** proposal, while not covering any product, addresses, for the first time, cybersecurity of the digital supply chain (of special importance in the case of the IoT) (recital 43 and Article 5(2a)).

- **Conformity Assessment**

Looking at the conformity assessment procedures, in general significant emphasis is put on the importance of standardisation in an effort to ensure greater conformity. In the context of this study, a comparative analysis of conformity assessment modules was done to elucidate the main approaches in view of studying the most similar and suitable modules for the planned initiative.

The GPSD and GPSR proposal opt for a presumption of safety in case common standards as specified in the Directive are applied. Similarly, the MDR (Article 7) and MR proposal (Article 17) adopt a presumption of conformity of machinery when manufacturers apply harmonised standards, with self-assessment through Module A provided as default option, but not for high-risk machinery.

In other cases, conformity assessment procedures as well as the involvement of third parties, greatly depends on the product classification adopted in the legislation: for instance, this is the case for the MDR (recital 60) as well as for the proposal on AI Act.

- **Market surveillance**

[138] This input was shared by Mark Whittle Director of CSES Europe, member of the Advisory Board.
[139] Including the natural or legal person who fully refurbishes a device.

Concerning market surveillance rules, the pieces of legislation analysed usually contain dedicated articles. However, it is worth mentioning that only some of them explicitly address certain aspects concerning post-market surveillance. This is particularly important when looking at new technologies, as these pose challenges related to the notion of placing a product on the market and the monitoring of its compliance with obligations and requirements post-market placement (i.e., life cycle approach). Products including new technologies can evolve and their safety features may change via software updates or machine learning after they have been placed on the market. For instance, AI Act proposal, sets out monitoring and reporting obligations for providers of AI systems regarding post-market monitoring and reporting, as well as the investigating of AI-related incidents and malfunctioning. Market surveillance authorities would also control the market and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market (Article 61).

It is worth mentioning that the new MSR,[140] which amended the 2008 market surveillance provisions under Regulation (EC) 765/2008, aims at reinforcing the effectiveness of market surveillance in the EU, with an eye on addressing challenges posed by the digital age. As set out in Article 2, the Regulation applies to all products that are subject to one of the 70 EU safety instruments listed in Annex I - including the RED, the MDR, the MD and the TSD - in the absence of more specific rules on market surveillance; however, the provisions requiring an EU-based economic operator.

[140] MSR: Regulation (EU) 2019/1020.

ANNEX 9: TABLE ILLUSTRATING THE POTENTIAL INTERPLAY BETWEEN A HORIZONTAL REGULATORY INTERVENTION (NOTABLY POLICY OPTION 4) WITH EXISTING PRODUCT-RELATED LEGISLATION

Legislation	Potential relationship between the existing product legislation and a comprehensive horizontal regulatory intervention (policy option 4)	Digital dimension	Cybersecurity elements covered	Possibility to opt for self-assessment when harmonised standards are applied	Modules	Types of products + other related remarks	Examples of types of products	NLF	Main relevant articles
Measuring Instruments - Directive 2014/32/EU	No amendments necessary, intervention to complement. Essential requirements for suitability and protection against corruption	yes	yes (measuring instruments have embedded software)	no	All except A1, C1	Measuring instruments	Water meters, gas meters, thermal energy meters, taximeters, automatic weighing instruments etc.	yes	17, 19(2), 30
Radio equipment - Directive 2014/53/EU + Delegated Regulation	RED DA to be implemented until the horizontal cybersecurity rules start applying. The upcoming legislation would then provide more specific cybersecurity requirements and it can be considered that the RED DA cybersecurity requirements would become	yes	yes	yes	A, B+C, H	All radio equipment	Wi-Fi routers, AM/FM radios, TVs, mobile phones, laptops, computers, RFID devices, navigation devices, radar (all devices using wireless communication such as LTE, 5G, Bluetooth, GPS, RFID etc.)	yes	3(3)(d)(e)(f) + DA (for scope and ER); 17 (conformity assessment)

	obsolete at the time when the horizontal legislation starts applying.								
Medical devices - Regulation (EU) 2017/745	out right exclusion of medical devices from the scope of the horizontal regulation due to more specific requirements set out in the medical devices regulation that are at least equivalent with the cybersecurity requirements in the intervention.	yes	yes	no	H1-like, B-like, D-like, F-like	Medical devices	High frequency ventilators, wearable automated external defibrillators, implantable pacemaker pulse-generator, coronary stents, cardiovascular catheters including guidewires and electrodes for electrophysiological diagnosis; Devices intended to remove undesirable substances out of the body, devices intended to separate cells by physical means, long term corrective contact	yes	52, Annexes IX - XI

							lenses, therapeutic devices intended to administer or exchange energy in a potentially hazardous way; Tracheostomy or tracheal tubes connected to a ventilator, short term corrective contact lenses, therapeutic devices intended to administer or exchange energy in a non-hazardous way, devices intended for recording X-Ray diagnostic images		
In vitro diagnostic medical devices - Regulation (EU) 2017/746	out right exclusion of medical devices from the scope of the horizontal regulation due to more specific requirements set out for in vitro diagnostic medical devices that are at least equivalent with the cybersecurity requirements of the intervention	yes	yes	no	B-like+D-like, H1-like	In vitro diagnostic medical devices	Reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, and accessories.	yes	48, Annexes IX - XI

Machinery Regulation – DRAFT COM(2021) 202	Complementarity, as MR covers cybersecurity with an impact on safety. The regulatory intervention would complement with requirements going beyond those having an impact on safety. Specific clarifications (provisions and recitals) could be considered to spell out the interplay between the two pieces of legislation, notably on aspects relating to safety (e.g. cross-referencing to application of Annex III relevant provision - e.g. 'protection against corruption')..	yes	yes	yes, as a rule (not for high-risk machinery)	Presumption of conformity of machinery when manufacturers apply harmonised standards; self-assessment by default option; third party assessment for high-risk machinery	Machinery products: (a) machinery; (b) interchangeable equipment; (c) safety components; (d) lifting accessories; (e) chains, ropes, slings and webbing; (f) removable mechanical transmission devices; (g) partly completed machinery; *Additionally, as compared to the current MD, the definition of safety component has been also clarified to include non-physical components such as software. A list of exclusions is also provided as in the current Machinery Directive, with few adjustments*	All machinery embedding AI systems ensuring safety functions and (non-embedded) AI ensuring a safety function in machinery	yes	Annex III, 21, 22

						(some changes on vehicles to ensure nothing is left out) and further clarifications (mainly when such products are covered by other legislation, such as motor/vehicles, electrical equipment designed for use within certain voltage limits, etc.)			
Toy Safety - Directive 2009/48/EU	Complementarity to RED and hence RED Delegated Regulation	yes	yes (very limited)	yes	Presumption of conformity for toys applying harmonised standards, self-assessment as default. Third-party notification when there are no standards, or not applied or published with restriction or upon choice of manufacturer	Toys for Children (<14)	AI-powered Toy Robots (e.g. Sphero, Cozmo, Hello Barbie)	yes	Annex I, 19

Machinery – Directive 2006/42/EU	Directive to be replaced by Regulation (see above)	yes	yes (e.g. limited references to h/w and s/w in control systems)	yes	Presumption of conformity of machinery when manufacturers apply harmonised standards; self-assessment by default option. For high-risk machinery (listed in Annex IV) where no harmonised standards exist, (a) the EC type-examination procedure, plus the internal checks on the manufacture of machinery OR (b) the full quality assurance procedure. *Note: High-risk machinery – listed in Annex I + COM empowerment for DA to update the list (if it poses a risk to human health taking into account its design and intended purpose + some criteria to establish that).*	Machinery products (incl. software ensuring safety functions, including AI systems) - '*safety component' means a physical or digital component, including software, of machinery which serves to fulfil a safety function and which is independently placed on the market, the failure or malfunction of which endangers the safety of persons but which is not necessary in order for the machinery to function or may be substituted by normal components in order for the machinery to function.*	(a) machinery; (b) interchangeable equipment; (c) safety components; (d) lifting accessories; (e) chains, ropes and webbing; (f) removable mechanical transmission devices; (g) partly completed machinery; *A list of exclusions is also provided a (mainly when such products are covered by other legislation, such as motor/vehicles, electrical equipment designed for use within certain voltage limits, etc.)*	yes	3(3), 12, 13, Annex I, Annexes VIII - X

Transportable pressure equipment - Directive 2010/35/EU	No amendments necessary, the regulatory intervention to complement. Essential requirements refer to requirements under ADR, RID and (Agreements on the carriage of dangerous goods by resp. road, rail or waterway), which seem to contain requirements linked to safety, and no specific cybersecurity requirements.	yes	no	no	type approval, supervision of manufacture, periodic/intermediate inspections and exceptional checks, initial inspections and tests, reassessment of conformity	Transportable pressure equipment	All pressure receptacles, their valves and other accessories + tanks, battery vehicles/wagons, multiple-element gas containers (MEGCs), their valves and other accessories	yes	2(15), 4, 13
Motor vehicles and their trailers - Regulation (EU) 2018/858	Out right exclusion from the scope of the horizontal regulation due to more specific cybersecurity requirements where compliance with a specific UN regulation is required (*UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to*	yes	yes	no	different forms of type-approval	Motor vehicles and their trailers	Motor vehicles, trailers, systems, components, separate technical units, parts, equipment	no	

	cybersecurity and cybersecurity management system [2021/387])								
Recreational craft and personal watercraft - Directive 2013/53/EU	No amendments necessary, intervention will complement.	yes	no	for some	A, A1, B+C, B+D, B+E, B+F, G, H, Post construction Assessment (PCA)	Recreational craft, personal watercraft, propulsions engines	Motorboats, sailboats, personal watercraft, propulsion engines, kill switches, steering wheels, fuel tanks, port lights	yes	20, 21, 22 - this choice is not understandable. Relevant for what?
Simple Pressure Vessels - Directive 2014/29/EU	No amendments necessary, intervention to complement.	no	no	no	B+C-like, B+C1, B+C2	Simple Pressure Vessels		yes	13
Non-automatic Weighing Instruments - Directive 2014/31/EU	No amendments necessary, intervention to complement. Some of the general requirements refer to issues related to cybersecurity such as prevention of fraudulent use.	yes	yes	no	B+D, B+F, D1, F1, G	Non-automatic weighing instruments		yes	13

Lifts - Directive 2014/33/EU	Interplay with the intervention depends on decided interplay with Machinery Directive /Machinery Regulation. Essential requirements (relating to health and safety) refer to Machinery Directive (Annex I of the MD; The essential health and safety requirements of point 1.1.2 of Annex I to Directive 2006/42/EC apply in any event.)	yes	yes [*to the extent of the scope of the Lifts Directive dealing with health and safety of lifts and safety components for lifts*]	no	B+C2, B+D, B+E, G, H, H1	Lifts, safety components for lifts	Lifts intended for the transport of persons, goods and fitted with controls inside the carrier; Safety components for lifts components for lifts listed in Annex III, e.g. devices for locking landing doors, overspeed limitation devices, safety circuits containing electronic components	yes	15, 16 1(3) in case of more specific Union law 6(1) as regards building interface including aspects related smart building systems if relevant 4, 5, 7, 8 Annex I: preliminary remarks 1 to 3, essential health and safety requirements 1.1 and all those related to regulating, controlling and monitoring of safety of lifts where interconnected programmable/smart functions can be used (analysis to be carried out on case-by-case)
Marine Equipment - Directive 2014/90/EU	No amendments necessary, intervention to complement.	yes	no	no	B+D, B+E, B+F, G	Marine equipment		yes	15
Cableway installations - Regulation (EU) 2016/424	No amendments necessary, intervention to complement. No specific cybersecurity requirements; essential requirement related to safety.	yes	no	no	B+D, B+F, G, H1	Subsystems of cableway installations; Safety components	Drives and brakes, cable winding gear, cableway vehicles, monitor and safety devices; Components intended to be incorporated into a subsystem or cableway for the	yes	18(2)

							purpose of ensuring a safety function		
Gas appliances - Regulation (EU) 2016/426	No amendments necessary, intervention to complement, depending on the interpretation of the scope of the mandatory risk assessment (see above). No specific cybersecurity requirements; general safety requirements and requirements linked to materials used, design and construction.	yes	not through specific requirements but products must be safe and correctly performing when normally used as regards risks due to use of gas as fuel	no	B+C2, B+D, B+E, B+F, G	appliances burning gaseous fuels; Safety devices	Gas cookers, ovens, space heaters, instantaneous and storage water heaters, camping lanterns, blow lamps, greenhouse heater, coffee machines gas fires, convector heaters, catalytic heater, air heaters, radiant heaters, boiler including district heating, boiler bodies, heat pumps, humidifiers, co-generation appliances, fuel cells, steam boiler units, refrigerators, deep freezers, air-conditioning units, washing machines, drying cabinets, tumble dryers, dish washing machines, ironing machines, appliance governors/appliance pressure regulators, multifunctional controls, burner control systems, etc.	yes	14(2)

Pressure equipment - Directive 2014/68/EU	No amendments necessary, intervention to complement. No specific cybersecurity requirements; requirements linked to safety.	yes	no	Only for products with limited pressure hazard (category I under PED)	All except A1, C1, F1; A only for products classified under PED as category I	In fact Essential Safety Requirements relate to the products, the category of the equipment determines the stringency of the conformity assessment procedure	Stationary pressure equipment such as storage vessels, piping, heat exchangers, boilers, ... The applications include consumers products (fire extinguishers, pressure cookers) but the main applications are industrial process systems (chemical, pharmaceutical, power industry)	yes	14 Why only Art. 14?
ATEX (equipment and protective systems intended for use in potentially explosive atmospheres - Directive 2014/34/EU	No amendments necessary, complementary and compatible with the horizontal initiative. ATEX Directive contains the provision of Annex II.1.5.8 on Risks arising from software. It states that: 'In the design of software-controlled equipment, protective systems and safety devices, special account must be taken of the risks arising from faults in the programme'.	yes	yes (limited only to some risks from software)	for some	A (only for some products), B+C1, B+D, B+E, B+F, G	Equipment Group I; Equipment Group II; Protective systems, Components	Equipment used in all premises where a potentially explosive atmospheres may appear, such as: coal an mining industry, petrochemical industry, agriculture, etc.	yes	4, 13, Annex I - why this choice? Relevant to what?

Personal protective equipment - Regulation (EU) 2016/425	No amendments necessary, intervention to complement; no cybersecurity (or even digital) element	Yes, for smart garments only	no	for PPE category I only	A (only for category I products), B+C, B+C2, B+D	Equipment providing protection to the user against different types of risk: category I; category II; category III	See Annex I of the PPE Regulation for PPE risk categories Category I PPE protect against low risks like superficial mechanical injury, atmospheric conditions that are not of an extreme nature, etc. Category II is all protective equipment (e.g. gloves, jackets, hats, glasses, masks, headphones) not covered under Category I or III Category III products are those who protect against at least one of the following risks: - substances and mixtures which are hazardous to health, - atmospheres with oxygen deficiency - harmful biological agent - ionizing radiation - high temperature environments (100°C) - low temperature environments (-50°C) - falling from a height; - electric shock and live working;	yes	15(2), 19

							- drowning; - cuts by hand-held chainsaws; - high-pressure jets; - bullet wounds or knife stabs; - harmful noise.		
Drones - Regulation 2018/1139, Implementing Regulation (EU) 2019/947 and Delegated Regulation	intervention to complement or to consider Drones Regulation as lex specialis.	yes	yes (limited)	for some	A (only for some products and if harmonised standards applied), B+C, H	Drones (unmanned aircraft systems)		yes *(Delegated Regulation*)	Delegated Regulation (EU) 2019/945 – Art. 13 and Annex (parts 7, 8, 9)

(EU) 2019/945									
Restriction of Hazardous Substances in Electrical and Electronic Equipment - Directive 2011/65/EU	No amendments necessary, intervention to complement; no cybersecurity (or even digital) element	no	N/A	yes	A	Restriction of use of hazardous substances in electrical and electronic equipment (EEE)	Lists restricted substances for EEE	yes	7(b)
Electromagnetic Compatibility - Directive 2014/30/EU	No amendments necessary, angle; EMCD applies to all (non-radio) electrical equipment. It is more over true for computers wired connected (without Wi-Fi, bluetooth...) by for example "Ethernet cables RJ45".	yes	N/A	yes	A, B+C	Any apparatus or fixed installation [radio equipment are excepted – as RED applicable]	E.g. Apparatus: induction hobs, microwave ovens, washing machines, vacuum cleaners, power tools, LED lights, witching power supply, solar panels. E.g. fixed installations: TV screens and signage, wind turbines, air conditioning systems, etc.	yes	14, 15(2), Annexes II, III, IV

Low Voltage - Directive 2014/35/EU	No amendments necessary, intervention to complement; Does not have a digital dimension. Furthermore, there is no empowerment for a delegated act to update the list of specific requirements in Annex I.	yes	N/A	yes	A	Electronic and electrical equipment (non-radio) within certain voltage limits	Household and similar electrical appliances, rotating electrical machines, cables, power supply units, laser equipment, circuit breakers, control gears, switchgears, capacitors, fuses, luminaires and lamps, etc. ==> not exclusively household application, several also have industrial application	yes	15(2), Annex III, Annex IV
Pyrotechnic Articles - Directive 2013/29/EU	No amendments necessary, intervention to complement. Does not have a digital dimension.	no	N/A	no	B+C2, B+D, B+E, G, H	Pyrotechnic articles	Any article containing explosive substances or an explosive mixture of substances designed to produce heat, light, sound, gas or smoke or a combination of such effects through self-sustained exothermic chemical reactions; e.g. fireworks, theatrical pyrotechnic articles, ignition devices, etc	yes	17, Annex I, Annex II
Civil Explosives - Directive 2014/28/EU	Intervention could complement. DA/IA empowerment to update list of	no	N/A	no	B+C2, B+D, B+E, B+F, G	Explosives for civil uses (pyrotechnic articles covered by Directive 2013/29/EU	Projectiles, grenades, smoke, certain types of fireworks, signals, etc.	yes	20

	essential or specific requirements, cyber elements could be potentially added on this legal basis for the safety angle); (Art 46, 48)-linked to safety					excluded)			
Noise emission in the environment by equipment for use outdoors - Directive 2000/14/EC	No amendments necessary, intervention to complement. There might be a digital dimension, but requirements under this Directive are limited only to noise emission requirements.	no (some of the equipment covered could have a digital dimension, but the directive's requirements are limited to noise emission)	N/A	yes	A-like, A2-like, G-like, H-like	Equipment for use outdoors. 57 equipment categories covered. 22 subject to noise limits and different conformity assessment procedures.	all machinery defined in Article 1(2) of Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 on the approximation of the laws of the Member States relating to machinery which is either self-propelled or can be moved and which, irrespective of the driving element(s), is intended to be used, according to its type, in the open air and which contributes to environmental noise exposure. E.g. tower cranes, motor hoes, hydraulic hammers, lawnmowers, piste caterpillars, etc.	No	14

Fertilisers – Regulation (EU) 2019/1009	No amendments necessary, intervention to complement.	no	N/A	for some	A (only for some products - depending on composition), A1, B+C, D1	Fertilising products	a substance, mixture, micro-organism or any other material, applied or intended to be applied on plants or their rhizosphere or on mushrooms or their mycosphere, or intended to constitute the rhizosphere or mycosphere, either on its own or mixed with another material, for the purpose of providing the plants or mushrooms with nutrient or improving their nutrition efficiency	yes	13, 15, Annex IV, Part I
Construction products - Regulation (EU) 305/2011	No amendments necessary, intervention to complement.	no	N/A	only self-assessment	Self-assessment as a rule (DoP). Production control and product testing; however, no correspondence with modules	Construction products	Any product or kit which is produced and placed on the market for incorporation in a permanent manner in construction works or parts thereof and the performance of which has an effect on the performance of the construction works with respect to the basic requirements for construction works	yes	4, 6, 28(2), 60, Annex V

Table 29: Table illustrating the potential interplay between a horizontal regulatory intervention with existing product-related legislation

ANNEX 10: EU FUNDING PROGRAMMES

The table below provides a list of relevant headings in EU funding programmes. These headings show how EU funding programmes will support SMEs and public authorities in implementing the measures to be taken under a possible horizontal regulatory initiative.

Digital Europe WP 2021-2022 Source: https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf	
Topic	**Indicative Budget in m EUR**
European Cyber Shield	
EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges	15
Uptake of innovative cybersecurity solutions in SMEs	32
Support to the health sector cybersecurity	10
Support to Implementation of relevant EU Legislation	
Deploying The Network Of National Coordination Centres With Member States (*Support through the Network of National Coordination Centres*)	27
Supporting the NIS Directive implementation and national cybersecurity strategies	20
Testing and certification capabilities	5
Total	109
Horizon Europe WP 2021-2022 Source: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf	
Topic	**Indicative Budget in m EUR**
Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity	21.5
Improved security in open-source and open-specification hardware for connected devices	18
AI for cybersecurity reinforcement	11
Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data	17
Secure and resilient digital infrastructures and interconnected systems	21.5
Hardware, software and supply chain security	18
Cybersecurity and disruptive technologies	11
Smart and quantifiable security assurance and certification shared across Europe	18
Total	**136**

Table 30: Relevant headings in EU funding programmes

ANNEX 11: THE NEW LEGISLATIVE FRAMEWORK (NLF)

Many products placed on the EU market have CE marking (CE) affixed to them. This marking is the visible symbol showing that the manufacturer has taken all necessary measures to ensure that the product complies with the applicable safety legislation. It plays a crucial part in the New Legislative Framework for the EU internal market for goods, which entered into force at the beginning of 2010. The New Legislative Framework is a blueprint for designing product regulation at EU level. It provides for the appropriate control of testing laboratories and certification bodies, and more importantly sets out a Union policy on surveillance of products on the market and of effective controls of products from third countries.

European product legislation was revolutionised by the "New Approach" introduced in 1985. The 'old approach' reflected the traditional manner in which national authorities drew up technical legislation, going into great detail – usually motivated by a lack of confidence in the rigour of economic operators on issues of public health and safety. This New Approach departs from this traditional approach and has become a role model for Better Regulation. So-called New Approach legislation sets out the levels of protection that must be achieved and does not pre-judge the choice of technical solutions to achieve the levels. Today, the New Approach directives cover a large proportion of products marketed in the EU in more than 20 industrial sectors, including electro-technical products, machinery, radio/telecoms equipment, toys, medical devices, construction products and high-speed rail systems. Most products covered by this legislation have CE marking affixed to them, which is the visible symbol that indicates that a product complies with all the applicable safety legislation.

A detailed description of the New Legislative Framework can be found in the Commission's 'Blue Guide' on the implementation of EU products rules.[141]

1. About the CE marking

The CE marking is required for the placing of the market of products falling under specific product categories and indicates that such products meet EU safety, health or environmental requirements. It guarantees the free movement of safe products within the European market and is a key indicator of a product's compliance with EU legislation.

The CE marking is affixed by the manufacturer to its products. By placing CE marking on a product, the manufacturer declares the product's conformity with the applicable legal requirements valid in Europe. It is the sole responsibility of manufacturers to verify that the goods they are selling comply with all relevant legislations or – if necessary – have to have it examined by a notified conformity assessment body for that purpose.

Not all products sold in the EU need to bear CE marking. CE marking applies to more than 20 different product categories, ranging from electrical equipment to toys and from explosives to medical devices. Each product falls under one or more Directives, which determine the specific requirements that the product must meet in order to be CE-marked. Only the product categories subject to specific directives are required to be CE marked.

Wholesalers and retailers also bear some responsibility: they must verify that all the goods they distribute which require a CE marking are actually carrying one and that the necessary controls have been carried out.

[141] European Commission (2016): "The 'Blue Guide' on the implementation of EU products rules 2016", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016XC0726%2802%29.

In order to avoid non-conformity abuses, legal measures and economic sanctions have been established to deter the vast majority from doing so.

2. Six steps to obtain the CE marking

To comply with legal requirements, manufacturers have to follow six necessary steps in order to make their products ready for the market:

1. **Identify the directive(s) and harmonised standards applicable to the product:** The essential requirements products have to fulfil (e.g. safety) are harmonised at EU level and are set out in general terms in the Directives. Harmonised European standards are issued with reference to the applied directives and express in detailed technical terms the essential requirements.
2. **Verify the product-specific requirements:** It is up the manufacturers to ensure that their products comply with the essential requirements of the relevant EU legislation. Full compliance of a product to the harmonised standards gives to the product the "presumption of conformity" with the relevant essential requirements. The use of harmonised standards remains voluntary as manufacturers may decide to choose other ways to fulfil the essential requirements.
3. **Identify whether an independent conformity assessment is required from a notified body:** Each directive covering a particular product specifies whether an authorised third party (notified Body) must be involved in the conformity assessment procedure necessary for CE marking.
4. **Test the product and check its conformity to the EU legislation:** One part of the procedure is a risk assessment. By applying the relevant harmonised European standards, the manufacturer will be able to fulfil the essential legislative requirements of the directives.
5. **Draw up and keep available the required technical documentation:** The manufacturer has to establish the technical documentation required by the Directive(s) for the assessment of the product's conformity to the relevant requirements and a risk assessment. Together with the declaration of conformity, the technical documentation must be presented on request to the competent national authorities.
6. **Affixing the CE mark to your product and Declaration of Conformity:** The CE marking must be affixed by the manufacturer, according to its legal format visibly, legibly and indelibly to the product or its data plate. If a Notified Body was involved in the production control phase, its identification number must also be displayed.

3. Conformity assessment

Conformity assessment is the process carried out by the manufacturer of demonstrating whether specified requirements relating to a product have been fulfilled. The legislator selects from the menu of conformity assessment procedures (laid down under Decision No 768/2008/EC) the most appropriate one(s) in order to address the specific needs of the concerned sector.

The following procedures are considered for policy options 3 and 4:

- **Internal production control ("self-assessment"):** The manufacturer himself ensures the conformity of the products to the legislative requirements.
- **Conformity assessment by a third party:** These third parties are laboratories, inspection and certification bodies which 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 since not all do. Accreditation is a formal system which provides an independent attestation of the competence, impartiality and integrity of conformity assessment bodies. The minimum criteria include competence, impartiality, integrity, etc. Notified bodies are private companies and operate in a competitive market.

4. Market surveillance

The enforcement of product safety legislation is an important task; not only to protect consumers and other users from unsafe products but also to ensure a level playing field for reputable businesses. In the EU market surveillance is the responsibility of the Member States, which establish market surveillance authorities for the different products covered by the 'New Legislative Framework. With the RAPEX system (see IP and Memo 10/130 on the 2009 Annual RAPEX Report) the European Union has an effective and efficient system in place to share information about dangerous products found on the European market.

3. Policy options 3 and 4 and the New Legislative Framework

Under policy options 3 and 4, the Commission would propose a regulation laying down cybersecurity requirements for products with digital elements. The intervention would be based on the New Legislative Framework's (NLF) blueprint for product regulation. In line with the NLF, it would lay down objective oriented cybersecurity requirements, leaving the technical details to European harmonised standards. It would also require manufacturers to carry out a conformity assessment, with self-assessment for the vast majority of products and third-party assessment by notified bodies for a small number of critical products. Member States would be required to designate notified bodies to carry out the procedures for conformity when a third party is required. They would also need to establish market surveillance authorities to prevent the making available on the market and use of non-compliant products.

Due to the nature of products with digital elements, policy options 3 and 4 will slightly adjust the "traditional" NLF approach in a number of ways:

- In the past, NLF legislation would lay down safety, health or environmental requirements. Policy options 3 and 4 will **introduce cybersecurity requirements**, which have so far not played any major role in NLF legislation (with the exception of the Radio Equipment Directive together with a recently adopted delegated regulation and a few safety-focused product regulation that partially take cybersecurity into account, such as the Toy Safety Directive).
- Most NLF legislation lays down requirements for tangible goods (such as toys or machinery). Policy options 3 and 4 would **introduce requirements for software as a non-tangible good**. While policy option 3 would only cover software embedded in hardware devices, policy option 4 would cover all software. The Radio Equipment Directive together with a recently adopted Delegated Regulation are also covering embedded software. In addition, the Medical Devices Regulation also covers software products.
- Unlike traditional NLF legislation, policy options 3 and 4 would not only lay down requirements for the placing on the market of products with digital elements but **cover the entire life cycle of such products**. Manufacturers will therefore be required to ensure that products are kept secure by issuing security updates for vulnerabilities discovered in their products. The whole life cycle approach is

necessary, as it is nearly impossible to develop products with digital elements that do not have any vulnerabilities at all.

ANNEX 12: ILLUSTRATION OF TWO-LEVEL RISK APPROACH TO CONFORMITY ASSESSMENT IN POLICY OPTION 4

Level of risk category	**Criteria of determining the risk level of the product**	**Type of product**	**Conformity assessment**	**European certification scheme on the basis of the Cybersecurity Act**
By default (for the vast majority of the products in the scope)	By default	All products with digital elements but those qualified as critical	Self-assessment (flexible approach – businesses can still choose third party)	Presumption of compliance with the horizontal requirements for the relevant category of products **Mandatory certification based on an available EU cybersecurity certification scheme for products could be considered, based on an empowerment for delegated act. The EU certification scheme would follow the relevant procedures of the Cybersecurity Act.*
Critical (narrow market share)	Functionality/ security-critical functions	Critical software, e.g. operating systems or firewalls	Third-party assessment	
	Intended or reasonably foreseeable use	Industrial control and automation systems used by entities		

Table 31: Illustration of a risk approach to conformity assessment in policy option 4

ANNEX 13: REGULATORY GAP ANALYSIS

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[142]) 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 products with digital elements, should entail as key minimum elements, (see *section 5.2)* that: (i) **cybersecurity is factored in the design and development** of the products with digital elements 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.

More specifically, such security requirements would include:

- aspects relating to the **properties of the products** such as: security by default; protection from unauthorised access; confidentiality and integrity of data, commands and programs; capability to perform or support integrity checks; availability of components against degradation and distributed denial of service attacks; protection of the exposed attack surfaces; enable adequate security updates.
- security **support** (i.e. **vulnerability handling, security updates, patching**) for the **whole life cycle (i.e. after the placement on the market)**, such as requirements to: identify dependencies and vulnerabilities, including composition of software used and supply chain-related information; have no known-vulnerabilities and address vulnerabilities without delay; test the security of the product with digital elements; have in place a process to quickly become aware of newly emerging vulnerabilities; ensure mechanisms allowing the secure updating; ensure that patches are delivered with advisory messages; have coordinated vulnerability disclosure policies.
- provision of **information and instructions** such as those concerning: contact information for reporting vulnerabilities; intended use, including the security environment foreseen; end of life of the product; security properties of the product; type of support offered and for how long; instructions on secure use and secure removal of data.

The following legislative gaps can be highlighted in both (A) general cybersecurity-related legislation and (B) product-related legislation:

A) **General cybersecurity-related legislation,** (including product-related) which is applicable across-sectors and/or across-products

- **The "NIS Directive"** or Directive concerning measures for a high common level of security of network and information systems across the Union (')[143], recently

[142] i.e. software that can be purchased by end users separately, such as operating systems; mobile apps; desktop applications; video games.

[143] Directive (EU) 2016/1148 (NIS Directive)

reviewed through the NIS2 Directive[144] imposes on entities operating in key sectors obligations of organisational and risk management nature, including due diligence supply chain security obligations.

- *Limitations:* These obligations do not entail requirements for the design or development or security support of products and can only have indirect effects in that regard.

- **General Data Protection Regulation (GDPR)[145]** lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
  - *Limitations:* It does not regulate the cybersecurity of products.
- The **Cybersecurity Act[146]** sets a framework for the development, at EU level, of voluntary certification schemes for specific ICT products, services and processes.
  - *Limitations:* While covering a similarly broad scope when it comes to products with digital elements as policy option 4, the Cybersecurity Act does not establish any mandatory cybersecurity requirements or legal obligations for placing products with digital elements on the market. Even if an EU certification scheme exists (currently 3 schemes are being developed)-, manufacturers do not have a legal obligation to seek certification for those products. A separate appropriate legislative framework would be required for such an end.

B) Product legislation

(i). General product legislation

- **General Product Safety framework**, i.e. the General Product Safety Directive (GPSD)[147], undergoing review through a General Product Safety Regulation (GPSR)[148] currently in the co-decision process[149]. It establishes requirements to ensure the safety of consumer products (both covered and not by harmonised legislation). The GPSR proposal states that cybersecurity risks that have an impact on the safety of consumers are covered by the concept of safety. The GSPR proposal clarifies[150] also that specific cybersecurity risks affecting the safety of consumers can be dealt with by sectorial [i.e. specific] legislation, GSPR acting as a **safety net** in case of gaps of such legislation.
  - *Limitations:* The generic requirement to factor in cybersecurity risks from the safety angle does not ensure *de jure* or *de facto* cybersecurity by design and by default of all these products throughout the lifecycle or any security

144 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final. The NIS2 Directive reached a provisional political agreement and is expected to be formally adopted by autumn 2022

145 Regulation 2016/679/EU.

146 Regulation (EU) 2019/881

147 Directive 2001/95/EC.

148 On 30 June 2021, the European Commission adopted a proposal for a new general product safety regulation, with a view of improving the safety of non-food consumer products on the internal market. Announced in the new consumer agenda strategy, the proposal aims to replace the current General Product Safety Directive

149 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council of 30 June 2021, COM(2021) 346 final.

150 Recital 22 of the GPSR proposal.

support. Even if some cybersecurity attacks could present a safety risk, this is far from comprehensive in terms of possible cybersecurity risks.

- **Product Liability framework**, i.e. the Product Liability Directive[151] currently under review, with a proposal due in autumn 2022. The product liability framework intervenes *ex post* by setting out liability rules for defective products so that consumers can claim compensation when a damage has been caused by defective products. More specifically, it establishes the right of injured persons to be compensated for damages caused by the defectiveness of a product. It 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'). The planned review of the product liability framework aims to update the definition of products, to also include software and to introduce, among others, liability for situations when damages are triggered by vulnerabilities after the placement of the product on the market, having regard to all circumstances.
  - *Limitations*: It does not set product requirements, let alone cybersecurity requirements for products. If a defective product with digital elements was not compliant with established cybersecurity requirements, this would be relevant in the damages case and trigger the liability of the manufacturer in question. Manufacturers cannot be held liable for how the product will be used, but they would have to comply with requirements that ensure security of the product regarding its design and development, make available information to the users on security features and functions and make available security support and relevant information in relation to that. 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. The product liability legislation is therefore **complementary and not substitutable to a legislation establishing product requirements**.

(ii). Sector or product-specific- New Legislative Framework (NLF) legislation and remaining 'old approach' legislation

- The NLF 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. It also typically provides for conformity assessment, which is the process conducted by the manufacturer to demonstrate whether specified requirements relating to a product have been fulfilled and provides for EU market surveillance under the responsibility of the Member States.
- 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 transport are still being regulated this way.
- Many of these sectors cover products that are not connected, and for which the cybersecurity angle is not applicable. For those products which are digital, the

[151] Directive 85/374/EEC.

current product-related legislation covers only certain aspects linked to the cybersecurity, if any, and, where applicable, only embedded software. Duty of care for whole lifecycle after the placement on the market, a key aspect for cybersecurity of products, is typically not covered by this type of legislation.

- A regulation of security of all software, including non-embedded, is a crucial missing aspect of the existing product legislation. Vulnerabilities in software are omnipresent and have cascading effects cross-sectors and borders. The examples of cyberattacks affecting software and the whole supply chain are abundant. Examples include 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; the Kaseya VSA supply chain attack, which used Kaseya's network administration software to attack over 1 000 companies, forcing a supermarket chain to close all its 500 shops across Sweden.

- As regards the overall interplay between NLF and 'old approach' legislation and any envisaged horizontal legislation establishing cybersecurity requirements for all products with digital elements, mention should be made that these would be complementary. The only potential outright exclusions (or *lex specialis* derogations) from the scope of a cybersecurity horizontal regulation would concern products (medical devices, cars) for which cybersecurity is regulated comprehensively in specific legislation on all key aspects (i.e. security in the design and properties of the product, whole life cycle, transparency and information). Even for those, cybersecurity requirements established by the horizontal regulation for standalone software, also upload-able on such products, would be complementary. A horizontal cybersecurity regulation on products with digital elements would not change the way products are placed on the internal market as per settled NLF, nor would it change the overall NLF governance setting (e.g. aspects such as market surveillance governance).

- The following product-specific pieces of legislation need particular attention because they are the only ones that cover cybersecurity aspects in a more detailed way :

a) **Radio Equipment Directive (RED)[152] and notably its Delegated Regulation[153]** establishes three essential security-related requirements for inter-connected radio equipment (i.e. wireless products): (i) ensure network protection; (ii) ensure safeguards for the protection of personal data and privacy, (iii) ensure protection from fraud.
   - *Limitations*: cover **only wireless products** (hardware and their embedded software). It does not cover wired-only connect products, nor non-radio components (e.g. processors). It **does not cover standalone (non-embedded) software**. Furthermore, the requirements are **very generic, not providing key specific cybersecurity requirements** that would guarantee security by design and default (e.g. no requirements are provided addressing cybersecurity risks to availability, integrity, confidentiality; vulnerability handling; transparency and recording of composition of products an supply chain, obligations for specific security-related information to users, etc.) **or obligations regarding security support for whole life cycle, i.e. after the**

152 Directive 2014/53/EU.
153 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.

placement on the market. *See also Annex 7 for a detailed comparison between the RED delegated act scope and requirements and those envisaged for a comprehensive horizontal cybersecurity regulation.*

b) **Machinery Directive[154] and proposal for a Machinery Regulation** proposed Regulation looks covers requirements and risks relating to and impacts on **safety**. It covers a certain category risks related to new digital technologies provoked by malicious third parties that have an impact on the safety of machinery products. It does not preclude the application to machinery products of other Union legislation specifically addressing cybersecurity aspects.

- *Limitations:* cybersecurity is only covered from a narrower angle, safety-related for a very specific category of machinery products/components. It does not cover non-embedded software in its scope, nor requirements of duty of care for whole life cycle.

c) **Medical Devices Regulation (MDR)[155] as well as the In Vitro Diagnostic Medical Devices Regulation[156]** contain requirements regarding devices, including on software and general obligations on manufacturers, covering the whole life cycle of products, as well as conformity assessment procedures.

- *Limitations:* the **scope is very narrow** limited to specific medical devices[157]. In relation to such specific legislation and in particular the specificity of cybersecurity requirements that cover key aspects, a potential comprehensive horizontal regulation setting out cybersecurity requirements could consider out rightly excluding such category of products from application.

d) **Regulation on motor vehicles[158] and Delegated Regulation**[159] requires vehicles to be protected against cyber-attacks. The Regulation empowers the Commission to develop detailed implementing rules. The Delegated Regulation introduces certain **cybersecurity requirements, including on software updates** and whole life cycle aspects, requiring compliance with specific UN regulations on technical specifications and cybersecurity[160] and providing for specific conformity assessment procedures.

- *Limitations:* the scope is **limited to vehicles**. In relation to such specific legislation, given the specificity of cybersecurity requirements that cover key aspects, a potential comprehensive horizontal regulation setting out cybersecurity requirements could consider **out rightly excluding** such category of products from application.

e) **Artificial Intelligence (AI) Act proposal** establishes, among others, requirements for high-risk AI systems. More specifically, the proposal requires high-risk AI systems to be designed and developed in such a way that they

154 Directive 2006/42/EC.
155 Regulation (EU) 2017/745.
156 Regulation (EU) 2017/746.
157 "For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation", Regulation (EU)2017/745, Annex I, Chapter II, REQUIREMENTS REGARDING DESIGN AND MANUFACTURE.
158 Regulation (EU) 2019/2144, https://eur-lex.europa.eu/eli/reg/2019/2144/oj.
159 Delegated Regulation (EU) 2022/545 supplementing Regulation 2019/2144; https://eur-lex.europa.eu/eli/reg_del/2022/545
160 UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387].

achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and **cybersecurity**, and perform consistently in those respects throughout their lifecycle. A risk management system is also required throughout their **entire lifecycle**, as well as regular systematic updating.

- *Limitations:* the **scope is very limited, i.e. high-risk AI systems** explicitly listed in the Act. The cybersecurity-related requirements are **generic**. Such legislation could be complementary to a comprehensive horizontal regulation introducing more specific cybersecurity requirements. Compliance with the latter could imply compliance with the high-level cybersecurity requirements of the former. A specific legal act is currently in preparation at Commission level aiming to harmonise certain national non-contractual civil liability rules, so as to ensure that injured persons claiming compensation for harm caused by AI system enjoy the same level of protection as injured persons claiming compensation for harm caused without the involvement of an AI system. These would therefore strengthen the leverage of the AI Act requirements, and potentially also of any more specific horizontal cybersecurity requirements.

EU legislation (in force, in adoption process or in preparation)	***How are cybersecurity-relevant aspects covered***	***What is missing?***
Horizontal/general EU legislation not product-relevant		
NIS Directive[161] (and upcoming NIS2)	*Covers measures for a high common cybersecurity level across the Union to increase the level of resilience of entities in a number of sectors or providing certain services considered key ('critical' aka 'essential' and/or 'important') across the Union.*	*The NIS Directive does not impose cybersecurity requirements on products..*
General Data Protection Regulation (GDPR)[162]	*Its scope is limited to the general protection of personal data.*	*It does not regulate cybersecurity of products and does not provide an adequate legal basis for this.*
Horizontal regulatory framework on products		
Cybersecurity Act[163]	*Introduces a framework to set certification mechanism for specific ICT products, services and processes.*	*There are currently not yet any EU cybersecurity certification scheme having been developed under the Cyber security Act (3 currently under development). Once in place, manufacturers will not have a legal obligation*

161 Directive (EU) 2016/1148
162 Regulation 2016/679/EU
163 Regulation (EU) 2019/881

EU legislation (in force, in adoption process or in preparation)	*How are cybersecurity-relevant aspects covered*	*What is missing?*
		to seek certification for their products. This framework, while it establishes cybersecurity objectives that can be (and in fact are to be) integrated in horizontal cybersecurity requirements for products with digital elements, does not establish any cybersecurity requirements or legal obligations for placing products with digital elements on the market. A separate appropriate legislative framework would be required for such an end.
General Products Safety Directive (GPSD)[164] undergoing review through a General Product Safety Regulation (GPSR)[165] currently in the co-decision process	*Its main purpose is to address product safety. In the GPSR proposal, cybersecurity risks that have an impact on the safety of consumers are covered by the concept of safety (i.e. appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product).*	*GPSR does not establish specific cybersecurity requirements for products.* *Even if cybersecurity attacks could present a safety risk, the focus of the GPSR would remain the safety in a more narrow sense.* *Compliance with specific horizontal cybersecurity requirements would entail compliance with the cybersecurity risk angle required for safety under GSPR, but not vice-versa. GSPR requirements are far insufficient to ensure security by design and by default of products.*
Directive on liability for defective products (the Product Liability Directive)[166] and upcoming review	*It governs the liability of the manufacturers for damage caused by the defectiveness of the product.* *The planned review of the product liability framework*	*It does not set product requirements, let alone cybersecurity requirements for products. Instead, it sets out liability rules for defective products so that*

164 Directive 2001/95/EC.

165 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council of 30 June 2021, COM(2021) 346 final.

166 Directive 85/374/EEC

EU legislation (in force, in adoption process or in preparation)	*How are cybersecurity-relevant aspects covered*	*What is missing?*
	aims to update the definition of products in line with other general product legislation, such as the product safety framework, to also include software and to introduce, among others, liability for situations when damages are triggered by lack of security updates which occurs after the placement of the product on the market, derogating from the general rule on product liability that considers only defectiveness present at the time when the product was placed on the market. *With the planned review, vulnerabilities in a product could be classified as a defect for which the manufacturer would have the obligation to take appropriate cybersecurity measures during the design, production.*	*consumers can claim compensation for damage caused by defective products. These can indeed have effects on the manufacturers' designing and development of products.* *Such a legislation is complementary and not substitutable to a legislation establishing product requirements.*
Union harmonisation legislation based on the New Legislative Framework (NLF)[167]		
Radio Equipment Directive (RED)[168] and relevant Delegated Regulation[169]	*RED governs the safety aspects of wireless connected products, entails the possibility for the Commission to impose security requirements on the manufacturer linked to the protection of personal data and privacy by means of delegated acts[170].* *The relevant delegated act establishes the following three essential security-related requirements for inter-connected radio equipment (i.e. wireless products): (i) ensure network protection; (ii) ensure safeguards for the*	*The security requirements cover only wireless products (hardware and their embedded software).* *They do not cover standalone (non-embedded) software.* *Furthermore, they are very generic, not providing key specific cybersecurity requirements that would guarantee security by design and default (e.g. no requirements are provided addressing cybersecurity risks to availability, integrity, confidentiality;*

167 Regulation (EC) 765/2008 and Decision No 768/2008/EC

168 Directive 2014/53/EU

169 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

170 See Article 3(3)(e)

EU legislation (in force, in adoption process or in preparation)	***How are cybersecurity-relevant aspects covered***	***What is missing?***
	protection of personal data and privacy, (iii) ensure protection from fraud.	*vulnerability handling; transparency and recording of composition of products an supply chain, obligations for specific security-related information to users, etc) or obligations regarding security support for whole life cycle, i.e. after the placement on the market.*
Machinery Directive[171] and proposal for a Machinery Regulation[172]	*The proposed Regulation provides that manufacturers shall be required to adopt proportionate measures which are limited to the protection of the safety of the machinery product. This does not preclude the application to machinery products of other Union legislation specifically addressing cybersecurity aspects.* *The proposed Regulation makes the link with the future cybersecurity schemes pursuant to the Cybersecurity Act for the purpose of demonstrating compliance with the future regulation on machinery products. In particular, in view of addressing the risks stemming from malicious third party actions that have an impact on the safety of machinery products, the proposed Regulation includes essential health and safety requirements for which a presumption of conformity may be given to the appropriate extent by a certificate or statement of conformity issued under a relevant cybersecurity scheme adopted pursuant to the Cybersecurity Act.*	*The proposed Regulation only covers a certain category of risks related to new digital technologies provoked by malicious third parties that have an impact on the safety of machinery products.* *It does not cover duty of care for whole lifecycle, nor standalone software*

171 Directive 2006/42/EC.
172 COM/2021/202 final.

EU legislation (in force, in adoption process or in preparation)	*How are cybersecurity-relevant aspects covered*	*What is missing?*
Medical Devices Regulation (MDR)[173] *and the* ***In Vitro Diagnostic Medical Devices Regulation***[174]	*It provides that for devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.* *Detailed guidelines on cybersecurity measures are in place, covering specific cybersecurity requirements, including duty of care throughout whole life cycle.*	*The scope is limited to specific medical devices*[175]*. It covers, supported by detailed guidelines, comprehensive cybersecurity requirements, including software (as well as some types of non-embedded software) and duty of care for whole life cycle.* *A potential horizontal regulation could consider exempting such category of products from application (similar to a lex specialis principle).*
Other product-specific ***NLF legislation*** *(see also Annex 9 of the draft IA report)*	*General safety-related requirements.*	*Only certain generic safety requirements are applicable; no specific cybersecurity requirements.* *No provisions on duty of care for whole life cycle.* *Standalone software not covered.*
Other product-specific legislation or legislative initiatives		
Regulation on motor vehicles[176] ***and Delegated Regulation*** *supplementing Regulation 2019/2144*[177]	*Cybersecurity is a precondition for consumer trust in* ***automated/connected vehicles****. Regulation (EU) 2144/2019 requires notably vehicles to be protected against cyber-attacks. The Regulation empowers the Commission to develop detailed implementing rules.* *The Delegated Regulation*	*The scope is limited to a category of products (connected vehicles), but the cybersecurity requirements are comprehensive.* *It does not cover cybersecurity requirements for standalone (non-embedded) software.* *A potential horizontal regulation could consider*

173 Regulation (EU) 2017/745.
174 Regulation (EU) 2017/746.
175 "For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation", Regulation (EU)2017/745, Annex I, Chapter II, REQUIREMENTS REGARDING DESIGN AND MANUFACTURE.
176 Regulation (EU) 2019/2144, https://eur-lex.europa.eu/eli/reg/2019/2144/oj.
177 Delegated Regulation (EU) 2022/545; https://eur-lex.europa.eu/eli/reg_del/2022/545

EU legislation (in force, in adoption process or in preparation)	*How are cybersecurity-relevant aspects covered*	*What is missing?*
	introduces certain cybersecurity requirements, including on software updates, requiring compliance with specific UN regulations on technical specifications and cybersecurity[178] *and providing for specific conformity assessment procedures.* *The car manufacturers are required to carry out a cybersecurity risk analysis and to put in place robust car design measures to avoid or to mitigate these risks.* *The Approval authority will verify the compliance of the vehicle by means of document checks and testing. Furthermore, in order to obtain a type approval, manufacturers will have to put in place a Cybersecurity Security Management System which will be certified by the vehicle approval authority. The Cybersecurity Security Management System is to ensure that the manufacturer has the effective internal processes in place to avoid cyberattacks during the whole lifetime of the vehicle (from the design to the end of life of a vehicle) to ensure monitoring of vulnerabilities of and cyber-attacks against its vehicles and to keep its risk assessment up to date.*	*exempting vehicles as regulated by this framework from application (similar to a lex specialis principle).*
Proposal for an ***Artificial Intelligence (AI) Act***[179] ***and upcoming AI liability rules***	*High-risk AI systems are required to be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity,*	*The scope is limited only to a certain type of products (high risk AI system).* *The cybersecurity requirements for the high-risk AI systems are generic*

178 UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387].

179 COM(2021)206

EU legislation (in force, in adoption process or in preparation)	*How are cybersecurity-relevant aspects covered*	*What is missing?*
	and perform consistently in those respects throughout their lifecycle. They are also required to establish, implement, document and maintain a risk management system throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating A risk-based approach is ensured in this regard (i.e. technical solutions aimed at ensuring cybersecurity must be appropriate to the relevant circumstances and the risks). *A specific piece of legislation is currently in preparation regarding specific liability aspects for AI systems. In particular, it aims to lay down rules on the burden of proof in the case of non-contractual fault-based civil law claims brought before national courts for damages caused by the output of an AI system or the failure of such a system to produce an output and on the disclosure of information to be documented or logged pursuant to [the AI Act], to enable a claimant to substantiate a claim for damages. This would concern all relevant provisions of the AI Act, including the cybersecurity obligations.*	*and not comprehensive.*

Table 32: Overview of EU legislation relevant for cybersecurity

ANNEX 14: STANDARDS RELATED TO PRODUCTS WITH DIGITAL ELEMENTS

Standards are technical means or specifications that are adopted by a recognised standardisation body. The key benefit of a standard is to build a common language and hence to ensure interoperability of products and services. In the EU, standards are voluntary and are developed by the industry and/or experts in the relevant field, either at their own initiative or at the request of a legislator.

In the case of European standardisation (EU Regulation 1025/2012), a harmonised European standard is a European standard developed at the request of the Commission by one of the European standardisation organisations (ESOs), in view of applying Union harmonisation legislation. Harmonised standards can be specific on how to implement the legislation, unlike essential requirements included in Union harmonisation legislation that are objective-oriented and technology-neutral.

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.), no piece of EU legislation requires currently comprehensive cybersecurity requirements for all products with digital elements, and hence no harmonised European standards for products with digital elements across sectors.

As in all product-specific legislation of the NLF type, a horizontal regulation setting out cybersecurity requirements for products with digital elements marketed in the Union would also be followed by a standardisation request. The Commission typically sends a request to European standardisation bodies to set out harmonised standards laying down the technical means through which the requirements set may be met.[180] Typically the standards start being developed in the transition period provided for by the regulation in question, which could be 2 years for application to start after the entry into force. This ensures that by the time of the application of the new rules, harmonised European standards are already in place *(see also section 5.2. and notably the presentation of options 3 and 4).* The harmonised standards can be developed taking account and building on existing European and international standards.

The adoption of harmonised European standards provides a key incentive for manufacturers to follow these standards and provides legal certainty to manufacturers, especially for SMEs. Even if European and international standards exist, it can be costly for businesses to identify relevant standards to meet adequate security requirements. Contractual or public procurement obligations or indirect effects stemming from supply chain security obligations can provide certain incentives for compliance with existing standards. However, without a common European understanding on which standards meet adequate security requirements, there is a risk of market fragmentation. A common understanding on standards can be defined through voluntary measures, such as public procurement guidelines or European certification. However, such voluntary measures would not provide sufficent leverage to systematically integrate security in all products with digital elements.

Considering the level of connectivity and inter-dependence of products with digital elements, a scattered approach relying on voluntary application of standards and indirect effects of other obligations or self-regulation would not effectively address the identified problems of low level of cybersecurity of products with digital elements in the internal market, nor the insufficient understanding among users of the security of products.

[180] REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation.

The table below presents an overview of existing standards and guidelines that touch upon cybersecurity of products with digital elements.

Standard	***Scope***
BSA	*Framework for Secure Software*[181]
ETSI EN 303 645	*Cyber Security for Consumer IoT: Baseline Requirements*[182]
ETSI TR 103 621	*Guide to Cyber Security for Consumer Internet of Things*[183]
ETSI TS 103 701	*Technical specification: Cyber Security Assessment for Consumer IoT*[184]
GSMA	*GSMA IoT Security Guidelines*[185]
GSMA	*IoT Security Guidelines for Endpoint Systems*[186]
ISA/IEC 62443 series	*Series of standards for Industrial Automation and Control System (IACS)*
IEC 62443 4-1	*Secure Product Development Lifecycle Requirements*[187]
IEC 62443 4-2	*Technical security requirements for IACS components*[188]
	Common Criteria[189]
ISO/IEC 5055	*Automated Source Code Quality Measures*[190]
ISO/IEC 27400:2022	*Cybersecurity - IoT Security and Privacy Guidelines*[191]
ISO/IEC 27034 series	*Information technology – Security techniques – Application Security*[192]
ISO/IEC 29147	*Information technology – Security techniques – Vulnerability disclosure*[193]
ISO/IEC 30111	*Information technology – Security techniques – Vulnerability handling processes*[194]
NIST	*Recommended Criteria for Cybersecurity Labelling for Consumer Internet of Things (IoT) Products*

181 https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
182 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
183 https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.01.01_60/tr_103621v010101p.pdf
184 https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
185 https://www.gsma.com/iot/resources/gsma-iot-security-guidelines-complete-document-set/
186 https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf
187 https://webstore.iec.ch/preview/info_iec62443-4-1%7Bed1.0%7Den.pdf
188 https://webstore.iec.ch/preview/info_iec62443-4-2%7Bed1.0%7Db.pdf
189 https://www.commoncriteriaportal.org/
190 https://www.iso.org/standard/80623.html
191 https://www.iso.org/standard/44373.html
192 https://www.iso.org/standard/44378.html
193 https://www.iso.org/standard/72311.html
194 https://www.iso.org/standard/69725.html

NIST SP 800-213	*IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*[195]
NIST SP 800-218	*Secure Software Development Framework (SSDF)*[196]
NISTIR 8259	*Foundational Cybersecurity Activities for IoT Device Manufacturers*[197]
NISTIR 8259A	*IoT Device Cybersecurity Capability Core Baseline*[198]
OWASP ISVS	*IoT Security Verification Standard*[199]
OWASP ASVS	*Application Security Verification Standard*[200]
OWASP SCVS	*Software Component Verification Standard*[201]
SAFECode	*Fundamental Practices for Secure Software Development*[202]

Table 33: Notable examples of relevant international standards, widely used industry best practices and guidelines

[195] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf
[196] https://csrc.nist.gov/publications/detail/sp/800-218/final
[197] https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers
[198] https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline
[199] https://owasp.org/www-project-iot-security-verification-standard/
[200] https://owasp.org/www-project-application-security-verification-standard/
[201] https://owasp.org/www-project-software-component-verification-standard/
[202] https://safecode.org/uncategorized/fundamental-practices-secure-software-development/