European Commission

Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715

Final Study Report

Written by

December 2021

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology

Directorate H: Digital Society, Trust and Cybersecurity

Unit H.2: Cybersecurity and Digital Privacy Policy

Contact: Jakub Boratynski

E-mail:Jakub.Boratynski@ec.europa.eu

European Commission

B-1049 Brussels

Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715

Final Study Report

Authors:

Stefan GEORGIEV (stefan.georgiev@wavestone.com)

Aude THIRRIOT (aude.thirriot@wavestone.com)

Carole MEZIAT (carole.meziat@wavestone.com)

Leonardo BARONE (leonardo.barone@wavestone.com)

Alessandro ZAMBONI (alessandro.zamboni@wavestone.com)

Adrien MERLIER (adrien.merlier@wavestone.com)

Facundo HERRERA (facundo.herrera@icf.com)

Ricardas JUSKEVICIUS (ricardas.juskevicius@icf.com)

Lorenzo PUPILLO (lorenzo.pupillo@ceps.eu)

Carolina POLITO (carolina.polito@ceps.eu)

Cristina DE LA MAZA (cmaza@carsa.es)

Audren LAYEUX (alayeux@carsa.es)

Pär WESTRÖM (pwestrom@carsa.es)

With the support of:

Tim WATSON

Maria LILLÀ MONTAGNANI

Gérôme BILLOIS

Framework Contract: SMART 2019/0024

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (http://www.europa.eu).

Luxembourg: Publications Office of the European Union, 2021

ISBN 978-92-76-45872-2

DOI 10.2759/025330

Printed in [Country]

□ PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

□ PRINTED ON TOTALLY CHLORINE-FREE BLEACHED PAPER (TCF)

□ PRINTED ON RECYCLED PAPER

□ PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

Table of Contents

Abbreviations

ADSL Asymmetric digital subscriber line

AI Artificial Intelligence

AIS Automatic identification system

API Application Programming Interface

ANSM Agence nationale de sécurité du médicament et des produits de santé

B2B Business to Business

B2C Business to Customers

CBA Cost-benefit Analysis

CCTV Closed-circuit television

COM Communication

CPC Central Product Classification

CRM Customer relationship management

CSA Cybersecurity Act

CSES Computer Science and Engineering Society

CWP Commission Work Program

DCS Distributed Control System

DECT Digital Enhanced Cordless Telecommunications

DG Directorate-General

DG CNECT Directorate-General for Communications Networks, Content and Technology

DG HOME Directorate-General for Migration and Home Affairs

DG GROW Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

DG JUST Directorate-General for Justice and Consumers

DG MOVE Directorate-General for Mobility and Transport

DG FISMA Directorate-General for Financial Stability, Financial Services and Capital Markets Union

DORA Digital Operational Resilience for the Financial Sector

DSRC Dedicated short-range communications

EC European Commission

ECG Electrocardiogram

ECSO European Cybersecurity Organisation

ECU Electronic Control Units

EDI Electronic data interchange

ENISA European Network and Information Security Agency

ERP Enterprise resource planning

EU European Union

FG Focus Group

GDPR General Data Protection Regulation

GPS Global Positioning System

GPSD General Product Safety Directive

HMI Human Machine Interface

HR Human Resources

IA Impact Assessment

ICS Industrial control system

ICT Information and Communication Technology

IDS Intrusion Detection System

INT Interview

IoT Internet of Things

IPS Intrusion Prevention System

ISA Information Sharing Agreements

ISIC International Standard Industrial Classification

JPO Japan Patent Office

LAN Local Area Networks

MES Manufacturing execution systems

MFA Multi-Factor Authentication

NACE Statistical classification of economic activities in the European Community

NAS Network-attached storage

NFC Near Field Communication

NOTICE National Operation Towards IoT Clean Environment

OECD Organisation for Economic Co-operation and Development

OTA Over The Air

PAN Personal Area Networks

PKI Public key infrastructure

PLC Programmable Logic Controller

RED Radio Equipment Directive

RF Radio frequency

RFID Radio-frequency identification

RTU Remote Transmission Unit

SAN Storage area network

SCADA Supervisory Control and Data Acquisition

SIEM Security Information and Event Management

SIM Subscriber identity module

SIS Safety Instrumented Systems

SLR Systematic Literature Review

SME Small Medium Entreprise

TCU Telematics control unit

TOS Terminal operating systems

USB Universal serial bus

VHF Very high frequency

VLAN Virtual Local Area Networks

VOIP Voice Over Internet Protocol

WLAN Wireless Local Area Networks

WS Workshop

Abstract

Over the past decades, ICT products have allowed our society to become smarter and more connected, offering new benefits to consumers while creating opportunities to businesses across the EU. Meanwhile, the pervasiveness of ICT products within the EU Single Market has brought forward unforeseen challenges not only to the users of such products but also to the society at large.

In recent years, the EU has undertaken several initiatives with the aim of improving the legislation around product cybersecurity. Nevertheless, the current EU legislative framework seems still to be incomplete in respect to ICT products cybersecurity. Furthermore, evidences suggest that the heterogeneity of ICT products does not allow to aggregate risk profiles per ICT product category and/or sector. Hence, it follows the need to define a set of essential cybersecurity requirements for all ICT products, applicable during the entire lifecycle.

Against this background, the study concludes that the horizontal legislation would represent the most cost-effective policy option, creating greater security in the Single Market while enhancing the business competitiveness, with both the sector specific and mixed approach being the second best. However, a more comprehensive and quantitative assessment of these policy options should be performed in a follow up study.

Executive summary

ICF, Wavestone, CARSA and CEPS were awarded the contract to carry out a "Study on the need of cybersecurity requirements for ICT products" – VIGIE 2020-0715. The study aims to explore the current state of cybersecurity in broad categories of Information Communication Technology (ICT) products, including non-embedded software, as well as to identify the reasons for the lack of sufficient security. Moreover, the study provides a thorough analysis of the current regulatory landscape with regard to cybersecurity requirements for ICT products and explores options for an appropriate intervention by the policy makers for addressing the constantly rising cybersecurity risks in the use of the ICT products. The study is conducted in compliance with the European Commission's Better Regulation Guidelines, primarily the guidelines on Impact Assessment, and Better Regulation Toolbox.

The objectives of this Study Report (D5) are:

1. To present the background and policy context of the study, and a number of elements for the description of the problem, and baseline scenario i.e. problem tree, hierarchy of policy objectives (general and specific objectives) constructed for the studied intervention. To present how they address the problem drivers, whether they are consistent with other EU policies and legislation, and discuss the rationale for EU action concerning the legal basis and subsidiarity principles.
2. To establish a definition and categorisation for ICT products and develop sample risk profiles; these can be further used to distinguish requirements according to risk profiles or evaluate the policy options by introducing differences based on risk profiles.
3. To propose a generic lifecycle for ICT products, as well as essential requirements and security requirements that stakeholders should fulfil during the entirety of the product's lifecycle.
4. To identify viable policy options, in addition to the baseline, to reach the objectives. This is achieved by mapping these options, and relevant policy measure against the New Legislative Framework (NLF), a toolbox of measures that improves market surveillance and boost quality of conformity assessment via product legislation. To analyse each policy option and ensure they are closely linked to the problem drivers and policy objectives.
5. To analyse the possible impacts according to key evaluation criteria (effectiveness and social impacts, efficiency and economic impacts, coherence, fundamental rights, EU added value, environmental impact, comparative assessment) and provide a comparative assessment of the policy options.

Background and policy context

ICT products have turned everything into something connected and smarter. Indeed, Smart Home, Smart Building, Smart Grid, Smart Factory and Connected Cars are now becoming a reality. However, while creating numerous opportunities for the European economy and society, digitalisation brings forward several new challenges. As emerging technologies invade both the personal and professional life of individuals, cyber threats increase every year. Consequently, the cybersecurity of ICT products becomes a paramount need for a prosperous European Digital Single Market.

In 2005, the European Commission recognised ICT products as powerful drivers of growth, thus highlighting the urgent need to build stakeholders' trust in technologies[1]. Since then, the European Union has striven to enhance cybersecurity within the Single Market. Particularly, the Cybersecurity Strategy of the European Union[2] put forward the policy responses available to Member States with the objective of tackling cyber threats and risks.

Furthermore, the Shaping Europe's Digital Future Strategy[3] called the attention once more on the risks and costs stemming from the pervasive use of new technologies. In the context of the new strategy, key initiatives are the establishment of a Joint Cybersecurity Unit, the revision of the NIS Directive, and giving a push to the Single Market for cybersecurity.

Moreover, the Council highlighted the need for a horizontal piece of legislation addressing all relevant aspects of the cybersecurity of ICT products and suggested to explore the connections between this piece of legislation and cybersecurity certification framework as defined in the Cybersecurity Act[4]. In the same way, the European Commission has also reiterated the commitment towards a more comprehensive approach to cybersecurity for connected products[5].

More recently, the European Parliament adopted a resolution calling the European Commission to explore the need for a horizontal piece of legislation mandating cybersecurity requirements for ICT products by 2023[6].

1. Methodological approach

The study relies upon literature review as well as primary data collection activities addressed to key stakeholder groups active in the field of cybersecurity (i.e. European Institutions and Agencies, Competent Authorities in Member States, ICT industry, Academic experts, and Professional and Consumer Associations).

As part of the targeted consultation activities, interviews, focus groups, targeted consultation, online survey and a series of workshops were conducted with the aim of presenting and discussing the findings of the study, as well as to gather stakeholders' views on the matter. The Project Team performed 52 interviews, nine focus groups and three workshops, collecting feedback from a great number of stakeholders across different stakeholder groups and EU Member States. In addition, a Delphi panel was conducted for the analysis of possible impacts of the policy options; the panel allowed the Project Team to collect feedback from 34 stakeholders. Lastly, the Project Team performed a targeted consultation (online survey) with all stakeholder groups across the EU from March 2021 to May 2021, gathering a total of 88 responses.

2. Problem definition

[1] European Commission (2005). Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions "I2010 – A European Information Society for growth and employment", COM(2005) 229 final. 1 June 2005, Brussels.

[2] European Commission (2013) Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, JOIN(2013) 1 Final,, Brussels.

[3] European Commission (2020). Shaping Europe's Digital Future, European Commission, 19 February 2020. Available at: https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_en

[4] European Council (2020). Council Conclusions on the cybersecurity of connected devices, 2 December 2020, Brussels.

[5] European Commission (2020). Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020 Brussels. JOIN(2020) 18 final. Brussels

[6] European Parliament (2021) The EU's Cybersecurity Strategy for the Digital Decade European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). P9_TA(2021)0286

In order to define the problem, the Project Team has performed a legislative gap analysis of existing EU laws related to cybersecurity requirements for ICT products. The analysis is demonstrated that the European legislative landscape is broad and comprehensive, but it does not target ICT products specifically. Particularly, the following conclusions shall be pointed out: (i) the current EU legislative framework does not cover all the security objectives set out in Art. 51 of the Cybersecurity Act; (ii) the legislation related to the NLF does not address fully the cybersecurity requirements for ICT products; (iii) the granularity of some of the requirements identified in the legislation does not guarantee the fulfilment of the security objectives and; (iv) some cybersecurity requirements addressed to service operators apply only indirectly to ICT products used to operate the service. At the same time, the analysis of national legislation shows – with some exceptions – that Member States are not planning to bring forward any legislative proposal that could enhance the cybersecurity of ICT products.

Additionally, following the desk research and stakeholder consultation activities, the Project Team has identified two main problems related to the cybersecurity of ICT products, namely the lack of secure ICT products across the EU (i.e. Problem 1) and the insufficient understanding among users of the level of cybersecurity for ICT products (i.e. Problem 2).

It is important to highlight that the analysis illustrates that insecure ICT products are not equally met across all sectors. Some sectors (e.g. energy, health) are characterised both by a more comprehensive sectoral legislation and by a higher attention and awareness from market operators towards cybersecurity aspects of ICT products. On the other hand, where specific sectoral provisions addressing cybersecurity concerns and cybersecurity requirements are lacking, and principles such as security by design or security-by-default principles are not guiding production, consumer devices appear to be more vulnerable to cyber-attacks.

Moreover, despite affecting both consumers and businesses, the analysis shows that the insufficient understanding about the level of cybersecurity for ICT products does not concern all users of ICT products in the same way. Users possess very different levels of IT skills and risk awareness. Hence, a clear differentiation on the term "users" should be made, distinguishing between regular and professional users.

Several root causes (i.e. problem drivers) lay behind the abovementioned problems. The data collection activities have highlighted the following problem drivers (i) the lack of qualified security professionals (i.e. developers), (ii) an unharmonized conformity assessment across the EU, (iii) the absence of rules for post-market surveillance, as well as of mandatory requirements (e.g. no clear obligations for the manufacturer) and, finally, (iv) the absence of a common legal basis setting cybersecurity requirements for ICT products. On the other hand, the information asymmetries between consumers and producers represent one of the main drivers for the insufficient understanding of the cybersecurity of ICT products among users. In fact, the cybersecurity aspects of ICT products are often not visible and understandable by the buyer (e.g. market for lemons), particularly when the buyer is a regular user.

These problem drivers, along with the others identified by this study, call for a general objective of increasing the level of cybersecurity of ICT products in the EU via the following specific policy objectives (SPOs):

- SPO 1: Set a common legal basis defining mandatory requirements, certification processes, risk assessment models and post market surveillance mechanisms.
- SPO 2: Define a mechanism that incentives manufacturers to produce more secure ICT products.
- SPO 3: Address cybersecurity at early stages of product development.

- SPO 4: Define comprehensive cybersecurity requirements for ICT products across all application domains.
- SPO 5: Promote cybersecurity curricular programmes for professional users.
- SPO 6: Setup a method to communicate to consumers the security level of ICT products.

These specific objectives address the key problems drivers and serve as the basis for the identification of the policy options.

3. Identification of ICT product categories and risk profiles

For the purpose of this study, the Project Team has proposed a classification of ICT Products. These can be ascribed into six generic indicative product categories: End devices, Software, Security, Programs for decision support, Networks, and Servers & systems. These categories were linked as far as possible to the five sectors covered by the study: Smart Manufacturing, Finance, Energy-Smart grid, Transport-Ports & Airports, and Smart Home.

Building on the EBIOS Risk Manager method, the Project Team has developed a method – applicable to all ICT products used within an economic sector – that enables the creation of risk profiles. Using desk research and experts' opinion, the Project Team used the adapted methodology to develop scenarios and risk-profiles for ICT Products. The results of the study also showed that it is not feasible to create aggregated risk profiles per ICT product category, or per sector due to the heterogeneity of ICT products within a category or a sector.

The risk profiles identified in this chapter can be considered as useful indicative findings for the establishment of Essential Requirements and security requirements for ICT products, as well as for defining the policy options, which can rely on different level of obligations based on the risk profiles.

4. Selection of cybersecurity requirements

Before proceeding with the definition of the cybersecurity requirements, some preliminary work was carried out. In particular, the lifecycle of an ICT product was defined to ensure cybersecurity is taken into account at all stages of the lifecycle. Indeed, both hardware and software – which may be present within the device natively or through additional non-embedded software, as well as on backend services – should be designed, produced, configured, maintained and decommissioned with security in mind, and security evaluation should always be part of the testing phases of the product.

The study identified eight Essential Requirements that can be used to set appropriate security levels for all ICT products. The Essential Requirements are defined as high-level security requirements that are to be applied to all products - and to services associated with such products, if any – and are not technology-specific.

In order to support the fulfilment of each Essential Requirement, the Project Team has identified a set of security requirements. These are associated to the risk profile of the ICT product and are meant to provide guidance on the measures to be applied to that ICT product on the basis of the risks this faces. A clear split of responsibilities between stakeholders involved with product security is needed, in order to ensure that the entire value chain follows the security requirements of the product seen as a system.

The study also provides a set of assessment activities to be performed depending on the risk profile of the ICT product. Such activities could support the conformity assessment of ICT products, to ensure their security before they are placed on the market but also apply to the development and provision of updates. The responsibility to perform conformity assessment activities between the manufacturer and third-party is likely to differ with the risk level. For example, ICT products facing high risks are more likely to be evaluated by third parties.

The Essential Requirements, security requirements and assessment activities are further used in the identification and evaluation of policy options, as they aim to be aligned with the NLF. They constitute a set of measures which is assumed to be used by the different policy options.

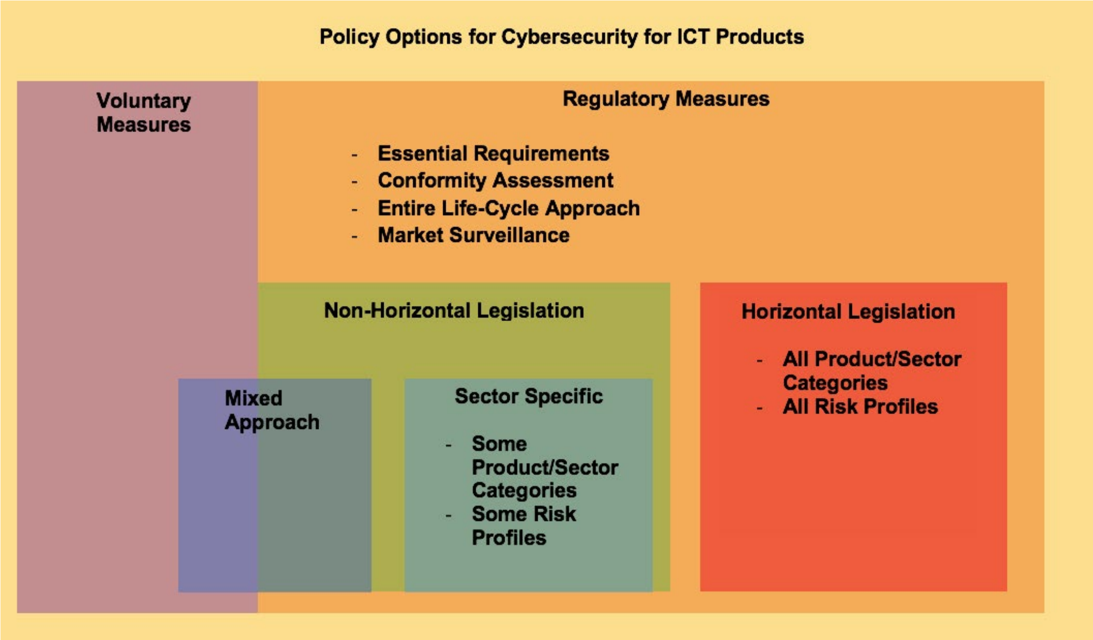
5. Identification of policy options

The Project Team has designed the policy options with reference to the NLF. The NLF can be considered as a toolbox of measures for use in product legislation. Therefore, to frame the different policy options, the Project Team has selected the main measures of the NLF to evaluate how they could be applied to cybersecurity for ICT products. In particular, the Project Team has focused on the Essential Requirements, the conformity assessment mechanisms, the reference to standards, and the provisions for market surveillance.

The Project Team has presented and elaborated on the following potential policy options (represented in Figure 1):

- Voluntary measures (Policy Option 1), involving current voluntary practices and measures to increase transparency and promote conformity assessments.
- Horizontal legislation (Policy Option 2), involving the implementation of a common regulatory approach applicable to all categories and risk profiles of ICT products.
- Sector-specific legislation (Policy Option 3), involving the implementation of a common regulatory approach applicable to specific ICT product / risk levels of sectors.
- Mixed approach (Policy Option 4), involving the implementation of a combination of regulatory and voluntary measures.

Figure 1 Overview of the Policy Options



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW

6. Analysis of the possible impacts

As a last step of this study, the Project Team has carried out an analysis of the impacts of the potential policy options which takes into account the key assessment criteria of effectiveness and social impacts, efficiency and economic impacts, coherence, fundamental rights, EU added value, and environmental impact. The analysis was based on the input of key stakeholders via the Delphi panel and the Targeted Consultation. Based on the results of the analysis, it was concluded that:

Horizontal legislation (Policy Option 2) is the most preferred policy option (please see Table 76 for the final score of the policy options). While, in comparison to the other policy options considered, Policy Option 2 may result in larger overall costs, its cost-effectiveness is also potentially the highest. Concerning effectiveness, horizontal legislation is likely to have the most positive impacts on the level of cybersecurity in ICT products, material and non-material safety, choice of reliable and secure ICT products and the trust in ICT products and the Digital Single Market. Concerning efficiency, Horizontal legislation is likely to have the most positive impacts on the competitiveness of the ICT industry, innovation in the ICT industry, functioning and harmonisation of the Internal Market, level playing field and the development of the Digital Single Market. Finally, it is expected to have positive impacts on coherence with other pieces of legislation (discussed in Chapter 2), fundamental rights, EU added value and environmental impact.

Horizontal Legislation would allow to harmonize the EU regulatory landscape and avoid overlapping requirements stemming from different pieces of legislation. In addition, Horizontal legislation is seen as creating greater security in the overall market as well as a better harmonization of the European single market, creating more viable conditions for operators aiming at entering the EU market. Furthermore, Horizontal legislation would allow to better tackle the problem drivers (policy issues) compared to the other policy options. For example, Horizontal legislation allows addressing the absence of mandatory requirements (e.g., no clear obligations for the manufacturer), or the absence of rules for post-market surveillance, with regards to cybersecurity.

The second-best options are found to be Sector-specific legislation (Policy Option 3) and the Mixed approach (Policy Option 4). They scored lower on all assessment aspects than the Horizontal legislation, but nevertheless received mostly positive feedback from the respondents. The key concern in relation to these two alternatives was associated with the possibility of fragmentation in cases of product-specific legislation, and uncertainty about the outcome of a final legislative mix.

The least preferred policy options are No action (Policy Option 0) and Voluntary approach (Policy Option 1). They are likely to have negligible or negative impacts on most of the assessment criteria. The main concerns from stakeholders relate to the need to regulate ICT products given their spread and potential security implications and that the voluntary measures are unlikely to be effective in this regard. They might have adverse impact on the functioning and harmonisation of the Internal Market and contribute little to the level playing field, competition and innovation in the European ICT industry (please see Chapter 6 for detailed discussion).

7. Conclusions and recommendations for EU Action

The results of the study point out that a horizontal legislation is expected to provide the best cost-effectiveness and overall best impact among the proposed policy options. The horizontal policy option was also among the favoured options for consulted stakeholders, with both the sector specific and mixed approach being the second best.

The follow-up of the study should focus on the performance of a more comprehensive and quantitative assessment of the policy options, together with a precise and robust impact analysis on the different measures proposed throughout the study (labelling, certification, essential requirements, etc.) to select the best combination of measures for a possible piece of legislation at EU level on ICT product cybersecurity.

Résumé

ICF, Wavestone, CARSA et CEPS ont obtenu le contrat pour réaliser une "Étude sur le besoin d'exigences de cybersécurité pour les produits TIC" - VIGIE 2020-0715. L'étude vise à explorer l'état actuel de la cybersécurité dans de grandes familles de produits appartenant aux technologies de l'information et de la communication (TIC), y compris les logiciels non-embarqués, ainsi qu'à identifier, le cas échéant, les raisons de l'absence d'une sécurité suffisante. En outre, l'étude fournit une analyse approfondie du paysage réglementaire actuel en ce qui concerne les exigences de cybersécurité pour les produits TIC, et explore les options pour une intervention appropriée par les décideurs politiques pour faire face à l'augmentation constante des risques de cybersécurité dans l'utilisation des produits TIC. L'étude est menée conformément aux Lignes directrices de la Commission Européenne sur l'amélioration de la réglementation, principalement les Lignes directrices sur l'analyse d'impact et la Boîte à outils pour une meilleure réglementation.

Les objectifs de ce rapport final (D5) sont les suivants :

1. Présenter l'historique et le contexte politique de l'étude, ainsi que le scénario de base et la description du problème, notamment via l'arbre des problèmes et la hiérarchisation des objectifs politiques (objectifs généraux et spécifiques) construits pour les mesures étudiées. Présenter comment ces objectifs adressent les causes du problème, s'ils sont cohérents avec les autres politiques et législations de l'UE, et discuter de la justification des actions de l'UE concernant la base juridique et les principes de subsidiarité.
2. Établir une définition et une catégorisation des produits TIC et développer des types de profils de risques ; ceux-ci pouvant être utilisés pour distinguer les exigences en fonction des profils de risques ou pour évaluer les options politiques en introduisant des différences basées sur les profils de risques.
3. Proposer un cycle de vie générique pour les produits TIC, ainsi que les exigences essentielles et les exigences de sécurité que les parties prenantes devraient remplir tout au long du cycle de vie du produit.
4. Identifier des options politiques viables, en plus des lignes directrices pour atteindre les objectifs. Pour ce faire, les options et les mesures politiques pertinentes sont mises en correspondance avec le Nouveau Cadre Législatif (NCL), une boîte à outils de mesures qui améliore la surveillance du marché et la qualité de l'évaluation de la conformité via la législation sur les produits. Analyser chaque option politique et s'assurer qu'elle est étroitement liée aux causes du problème et aux objectifs politiques.
5. Analyser les impacts possibles selon des critères d'évaluation clés (efficacité et impacts sociaux, efficience et impacts économiques, cohérence, droits fondamentaux, valeur ajoutée pour l'UE, impact environnemental, évaluation comparative) et fournir une évaluation comparative des différentes options politiques.

Historique et contexte politique

Les TIC ont transformé tous les produits en outils connectés et intelligents : la maison intelligente, le bâtiment intelligent, le réseau électrique intelligent, l'usine intelligente et les voitures connectées deviennent maintenant une réalité. Cependant, tout en créant de nombreuses opportunités pour l'économie et la société européennes, la numérisation crée plusieurs nouveaux défis. Alors que les technologies émergentes envahissent la vie personnelle et professionnelle des individus, les cybermenaces augmentent chaque année. Par conséquent, la cybersécurité des produits TIC devient un besoin primordial pour un Marché Numérique Unique européen prospère.

En 2005, la Commission Européenne a reconnu que les produits TIC étaient de puissants moteurs de croissance, soulignant ainsi le besoin urgent de renforcer la confiance des parties prenantes dans ces technologies[1]. Depuis lors, l'Union Européenne s'est efforcée de renforcer la cybersécurité au sein du Marché Unique. En particulier, la stratégie de l'Union Européenne en matière de cybersécurité[2] a présenté les réponses politiques dont disposent les États Membres pour faire face aux menaces et aux risques de cybersécurité.

En outre, la stratégie "Donner forme à l'avenir numérique de l'Europe"[3] a attiré une fois de plus l'attention sur les risques et les coûts induits par l'utilisation généralisée des nouvelles technologies. Dans le contexte de la nouvelle stratégie, les initiatives clés sont la création d'une unité conjointe de cybersécurité, la révision de la Directive NIS et l'impulsion donnée au Marché Unique de la cybersécurité.

De plus, le Conseil a souligné la nécessité d'un texte législatif horizontal couvrant tous les aspects pertinents de la cybersécurité des produits TIC et a suggéré d'explorer les liens entre ce texte législatif et le cadre de certification de la cybersécurité tel que défini dans le Règlement sur la cybersécurité[4]. De la même manière, la Commission Européenne a également réitéré son engagement en faveur d'une approche plus globale de la cybersécurité des produits connectés[5].

Plus récemment, le Parlement européen a adopté une résolution invitant la Commission Européenne à étudier la nécessité d'un texte législatif horizontal imposant des exigences de cybersécurité pour les produits TIC d'ici 2023[6].

1. Approche méthodologique

L'étude s'appuie sur une analyse documentaire ainsi que sur des activités de collecte de données primaires adressées aux principaux groupes de parties prenantes actifs dans le domaine de la cybersécurité (c'est-à-dire les institutions et agences européennes, les autorités compétentes des États Membres, le secteur des TIC, les experts universitaires et les associations professionnelles et de consommateurs).

Dans le cadre des activités de consultation ciblée, des entretiens, des groupes de discussion, une enquête en ligne et une série d'ateliers ont été menés dans le but de présenter et de discuter les résultats de l'étude, ainsi que de recueillir les points de vue des parties prenantes sur la question. L'équipe de projet a réalisé 52 entretiens, neuf groupes de discussion et trois ateliers, recueillant ainsi les réactions d'un grand nombre de parties prenantes de différents groupes et États membres de l'UE. En outre, un panel Delphi a été organisé pour l'analyse des impacts possibles des différentes options politiques ; ce panel a permis à l'équipe projet de recueillir les réactions de 34 parties prenantes. Enfin, l'équipe de projet a réalisé une consultation ciblée (enquête en ligne) auprès de tous les groupes de parties prenantes à travers l'UE de mars 2021 à mai 2021, recueillant un total de 88 réponses.

2. Définition du problème

Afin de définir le problème, l'équipe projet a effectué une analyse des lacunes législatives des lois européennes existantes relatives aux exigences de cybersécurité pour les produits TIC. L'analyse a démontré que le paysage législatif européen est vaste et complet, mais qu'il ne cible pas spécifiquement les produits TIC. En particulier, les conclusions suivantes ont été mises en avant : (i) le cadre législatif européen actuel ne couvre pas tous les objectifs de sécurité énoncés à l'art. 51 du Règlement pour la cybersécurité ; (ii) la législation relative au NCL ne traite pas pleinement des exigences de cybersécurité pour les produits TIC ; (iii) la granularité de certaines des exigences identifiées dans la législation ne garantit pas le respect des objectifs de sécurité et ; (iv) certaines exigences de cybersécurité adressées aux opérateurs de services ne s'appliquent qu'indirectement aux produits TIC utilisés pour exploiter le service. Dans le même temps, l'analyse des législations nationales montre - à quelques exceptions près

- que les États membres ne prévoient pas de présenter de proposition législative susceptible de renforcer la cybersécurité des produits TIC.

En outre, à la suite des recherches documentaires et des activités de consultation des parties prenantes, l'équipe projet a identifié deux problèmes principaux liés à la cybersécurité des produits TIC, à savoir le manque de produits TIC sécurisés dans l'UE (problème 1) et une insuffisante compréhension par les utilisateurs du niveau de cybersécurité des produits TIC (problème 2).

Il est important de souligner que l'analyse montre que les produits TIC non sécurisés ne sont pas rencontrés de manière égale dans tous les secteurs. Certains secteurs (par exemple, l'énergie et la santé) se caractérisent à la fois par une législation sectorielle plus complète et par une plus grande attention et sensibilisation des opérateurs du marché aux aspects de cybersécurité des produits TIC. En revanche, lorsque des dispositions sectorielles spécifiques traitant des préoccupations et des exigences en matière de cybersécurité font défaut et que des principes tels que la sécurité dès la conception ou la sécurité par défaut ne guident pas la production, les appareils grand public semblent plus vulnérables aux cyberattaques.

En outre, bien qu'elle touche à la fois les consommateurs et les entreprises, l'analyse montre qu'une insuffisante compréhension du niveau de cybersécurité des produits TIC ne concerne pas tous les utilisateurs de ces produits de la même manière. Les utilisateurs possèdent des niveaux très différents de compétences informatiques et de sensibilisation aux risques. Il convient donc de différencier clairement le terme "utilisateurs", en distinguant les utilisateurs grand public des utilisateurs professionnels.

Il existe plusieurs causes racines aux problèmes susmentionnés. Les activités de collecte de données ont mis en évidence les facteurs suivants (i) le manque de professionnels qualifiés en matière de sécurité (c'est-à-dire de développeurs), (ii) une évaluation de la conformité non harmonisée dans l'UE, (iii) l'absence de règles pour la surveillance après la mise sur le marché, ainsi que d'exigences obligatoires (par exemple, aucune obligation claire pour le fabricant) et, enfin, (iv) l'absence d'une base juridique commune fixant des exigences de cybersécurité pour les produits TIC. D'autre part, les asymétries d'information entre les consommateurs et les fabricants constituent l'un des principaux facteurs expliquant la compréhension insuffisante de la cybersécurité des produits TIC par les utilisateurs. En réalité, les aspects de cybersécurité des produits TIC ne sont souvent pas visibles et compréhensibles par l'acheteur (similaire au « *market for lemons*»), en particulier lorsque l'acheteur est un utilisateur grand public.

Ces causes racines, ainsi que les autres identifiées par cette étude, appellent à un objectif général d'augmentation du niveau de cybersécurité des produits TIC dans l'UE via les Objectifs Politiques Spécifiques (OPS) suivants :

- OPS1 : Etablir une base juridique commune définissant les exigences obligatoires, les processus de certification, les modèles d'évaluation des risques et les mécanismes de surveillance post-marché.
- OPS 2 : Définir un mécanisme qui incite les fabricants à produire des produits TIC plus sûrs.
- OPS 3 : Aborder la cybersécurité dès les premières étapes du développement des produits.
- OPS 4 : Définir des exigences complètes en matière de cybersécurité pour les produits TIC dans tous les domaines d'application.
- OPS 5 : Promouvoir des programmes d'enseignement de la cybersécurité pour les utilisateurs professionnels.

- OPS 6 : Mettre en place une méthode pour communiquer aux consommateurs le niveau de sécurité des produits TIC.

Ces objectifs spécifiques répondent aux principaux facteurs de problèmes et servent de base à l'identification des options politiques.

3. Identification des catégories de produits TIC et des profils de risques

Pour les besoins de cette étude, l'équipe projet a proposé une classification des produits TIC. Ceux-ci peuvent être répartis en six catégories de produits génériques indicatifs : Appareils terminaux, Logiciels, Sécurité, Programmes d'aide à la décision, Réseaux, et Serveurs & systèmes. Ces catégories ont été reliées autant que possible aux cinq secteurs couverts par l'étude : *Smart manufacturing*, Finance, Energie, Transports (ports et aéroports), et *Smart Home*.

En s'appuyant sur la méthode EBIOS Risk Manager, l'équipe projet a développé une méthode – applicable à tous les produits TIC utilisés d'un secteur économique – qui permet de créer des profils de risques. En s'appuyant sur des recherches documentaires et des avis d'experts, l'équipe projet a utilisé la méthodologie adaptée pour développer des *scénarii* et des profils de risques pour les produits TIC. Les résultats de l'étude ont également montré qu'il n'est pas possible de créer des profils de risques agrégés par catégorie de produits TIC, ou par secteur, en raison de l'hétérogénéité des produits TIC au sein d'une catégorie ou d'un secteur.

Les profils de risques identifiés dans ce chapitre peuvent être considérés comme des résultats indicatifs utiles pour l'établissement des exigences essentielles et des exigences de sécurité pour les produits TIC, ainsi que pour la définition des options politiques, qui peuvent reposer sur différents niveaux d'obligations en fonction des profils de risques.

4. Sélection des exigences de cybersécurité

Avant de procéder à la définition des exigences de cybersécurité, certains travaux préliminaires ont été réalisés. En particulier, le cycle de vie d'un produit TIC a été défini afin de s'assurer que la cybersécurité est prise en compte à toutes les étapes du cycle de vie. En effet, tant le matériel que les logiciels – qui peuvent être présents dans l'appareil de manière native ou par le biais de logiciels supplémentaires non embarqués, ainsi que dans les services *backend* – doivent être conçus, produits, configurés, maintenus et mis hors service en tenant compte de la sécurité, et l'évaluation de la sécurité doit toujours faire partie des phases de test du produit.

L'étude a identifié huit exigences essentielles qui peuvent être utilisées pour définir des niveaux de sécurité appropriés pour tous les produits TIC. Les exigences essentielles sont définies comme des exigences de sécurité de haut niveau qui doivent être appliquées à tous les produits – et aux services associés à ces produits, le cas échéant – et ne sont pas spécifiques à une technologie.

Afin de mettre en place chaque exigence essentielle, l'équipe projet a identifié un ensemble d'exigences de sécurité. Celles-ci sont adaptées au profil de risques du produit TIC et sont destinées à fournir des conseils sur les mesures à appliquer au produit TIC en fonction des risques auxquels il est sujet. Une répartition claire des responsabilités entre les parties prenantes impliquées dans la sécurité des produits est nécessaire, afin de garantir que l'ensemble de la chaîne de valeur respecte les exigences de sécurité du produit considéré comme un système dans son ensemble.

L'étude fournit également une série d'activités d'évaluation à réaliser en fonction du profil de risques du produit TIC. Ces activités permettent l'évaluation de la conformité des produits TIC, afin de garantir leur sécurité avant leur mise sur le marché. Elles incluent également le développement et la mise à disposition de mises à jour. Le niveau de répartition des responsabilités des activités d'évaluation de la conformité entre le fabricant et le tiers est susceptible de varier en fonction du niveau de risque. Par exemple, les produits TIC présentant des risques élevés sont plus susceptibles d'être évalués par des tiers.

Pour s'aligner avec le NCL, l'identification et l'évaluation des options politiques s'appuient également sur les exigences essentielles, les exigences de sécurité et les activités d'évaluation. Ces dernières constituent un ensemble de mesures qui sont supposées être utilisées par les différentes options politiques.

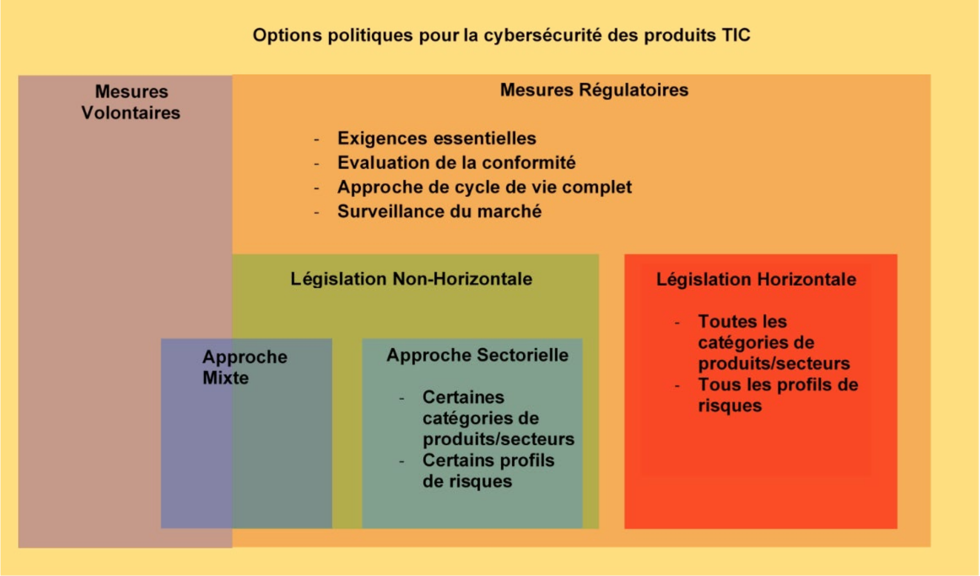
5. Identification des options politiques

L'équipe projet a conçu les options politiques en se référant au NCL. Le NCL peut être considéré comme une boîte à outils de mesures à utiliser dans la législation sur les produits. Par conséquent, pour encadrer les différentes options stratégiques, l'équipe projet a sélectionné les principales mesures du NCL pour évaluer comment elles pourraient être appliquées à la cybersécurité des produits TIC. En particulier, l'équipe projet s'est concentrée sur les exigences essentielles, les mécanismes d'évaluation de la conformité, la référence aux normes et les dispositions relatives à la surveillance du marché.

L'équipe projet a présenté et élaboré les options politiques potentielles suivantes (représentées dans la Figure 2) :

- Mesures volontaires (option politique 1), impliquant les pratiques volontaires actuelles et les mesures visant à accroître la transparence et à promouvoir les évaluations de la conformité.
- Législation horizontale (option politique 2), impliquant la mise en œuvre d'une approche réglementaire commune applicable à toutes les catégories et à tous les profils de risques des produits TIC.
- Législation sectorielle (option politique 3), impliquant la mise en œuvre d'une approche réglementaire commune applicable à des produits TIC spécifiques / niveaux de risque des secteurs.
- Une approche mixte (option politique 4), impliquant la mise en œuvre d'une combinaison de mesures réglementaires et volontaires.

Figure 2 Aperçu des options politiques


Options politiques pour la cybersécurité des produits TIC
Mesures Volontaires
Mesures Régulatoires
- Exigences essentielles
- Evaluation de la conformité
- Approche de cycle de vie complet
- Surveillance du marché
Législation Non-Horizontale
Législation Horizontale
- Toutes les catégories de produits/secteurs
- Tous les profils de risques
Approche Mixte
Approche Sectorielle
- Certaines catégories de produits/secteurs
- Certains profils de risques

SOURCE: ETUDE SUR LE BESOIN D'EXIGENCE DE CYBERSÉCURITÉ POUR LES PRODUITS TIC (2021), ÉLABORATION DES AUTEURS SUR LA BASE D'UNE ANALYSE DOCUMENTAIRE

6. Analyse des impacts possibles

Comme dernière étape de cette étude, l'équipe projet a effectué une analyse des impacts des options politiques potentielles qui prend en compte les critères d'évaluation clés de l'efficacité et des impacts sociaux, de l'efficience et des impacts économiques, de la cohérence, des droits fondamentaux, de la valeur ajoutée de l'UE et de l'impact environnemental. L'analyse s'est appuyée sur les contributions des principales parties prenantes via le panel Delphi et la consultation ciblée. Sur la base des résultats de l'analyse, il a été conclu que :

La législation horizontale (option politique 2) est l'option politique la plus plébiscitée (veuillez consulter le Table 76 pour le score final des options politiques). Si, par rapport aux autres options stratégiques envisagées, l'option 2 peut entraîner des coûts globaux plus élevés, son rapport coût-efficacité est aussi potentiellement le meilleur. En ce qui concerne l'efficacité, la législation horizontale est susceptible d'avoir les effets les plus positifs sur le niveau de cybersécurité des produits TIC, la sécurité matérielle et immatérielle, le choix de produits TIC fiables et sûrs et la confiance dans les produits TIC et le Marché Unique Numérique. En ce qui concerne l'efficience, la législation horizontale devrait avoir les effets les plus positifs sur la compétitivité du secteur des TIC, l'innovation dans ce secteur, le fonctionnement et l'harmonisation du marché intérieur, l'égalité des conditions de concurrence et le développement du Marché Unique Numérique. Enfin, elle devrait avoir des effets positifs sur la cohérence avec d'autres textes législatifs (examinés au chapitre 2), les droits fondamentaux, la valeur ajoutée de l'UE et l'impact environnemental. La législation horizontale permettrait d'harmoniser le paysage réglementaire de l'UE et d'éviter le chevauchement d'exigences découlant de différents textes législatifs. En outre, la législation horizontale est considérée comme créant une plus grande sécurité sur le marché global ainsi qu'une meilleure harmonisation du Marché Unique Européen, créant des conditions plus viables pour les opérateurs visant à entrer sur le marché de l'UE. En outre, la législation horizontale permettrait de mieux s'attaquer aux causes du problème (questions politiques) par rapport aux autres options politiques. Par exemple, la législation horizontale permet de remédier à l'absence d'exigences obligatoires (par exemple, pas d'obligations claires pour le fabricant), ou à l'absence de règles pour la surveillance post-commercialisation, en ce qui concerne la cybersécurité.

Les deuxièmes meilleures options sont la législation sectorielle (option 3) et l'approche mixte (option 4). Elles ont obtenu des résultats inférieurs à ceux de la législation horizontale sur tous les aspects de l'évaluation, mais ont néanmoins reçu des commentaires majoritairement positifs de la part des répondants. Pour ces deux options, les principales préoccupations étaient liées à la fragmentation potentielle sur le marché en cas de législation spécifique à un produit et l'incertitude des résultat d'une approche mixte d'interventions publiques.

Les options politiques les moins appréciées sont l'absence d'action (option politique 0) et l'approche volontaire (option politique 1). Elles sont susceptibles d'avoir des effets négligeables ou négatifs sur la plupart des critères d'évaluation. Les principales préoccupations des parties prenantes portent sur la nécessité de réglementer les produits TIC compte tenu de leur diffusion et de leurs implications potentielles en matière de sécurité, et sur le fait que les mesures volontaires ont peu de chances d'être efficaces à cet égard. Elles pourraient avoir un impact négatif sur le fonctionnement et l'harmonisation du marché intérieur et peu contribuer à l'égalité des conditions de concurrence, à la concurrence et à l'innovation dans l'industrie européenne des TIC (voir le chapitre 6 pour plus de détails).

7. Conclusions et recommandations pour l'action de l'UE

Les résultats de l'étude montrent qu'une législation horizontale devrait offrir le meilleur rapport coût-efficacité et le meilleur impact global parmi les options politiques proposées. L'option horizontale figure également parmi les options préférées des parties prenantes consultées, elle-même suivie de l'approche sectorielle et de l'approche mixte, apparaissant en second choix d'après les résultats de l'étude.

Les suites à donner à cette étude devront se concentrer sur la réalisation d'une évaluation plus complète et quantitative des options politiques, ainsi que sur une analyse d'impact précise et solide des différentes mesures proposées tout au long de l'étude (label, certification, exigences essentielles, etc.) afin de sélectionner la meilleure combinaison de mesures pour une potentielle législation à l'échelle de l'UE concernant la cybersécurité des produits TIC.

Introduction

This Final Study Report D5 aims to summarise the work done during the Study on the need of Cybersecurity requirements for ICT products. The study supports the work of the European Commission by exploring the current state of cybersecurity for ICT products. The study provides an in-depth analysis of the current regulatory framework with regard to cybersecurity requirements for ICT products, identifying the reasons underpinning the lack of adequate security to cyberthreats of these products. It also selects and explores the possible options for an appropriate intervention by the policy makers to address the gaps in the regulatory environment covering ICT products.

The report is framed by Tool #52 from the Better Regulation Guidelines[7], building on the evidence collected in the problem definition, categorisation of ICT products and risk profiles, and cybersecurity requirements for identified risk profiles in order to identify the policy options and assess the possible impacts.

Chapter 1: Scope and methodology

The scope and methodology Chapter outlines the six core objectives of the study, as well as the methodology and tools which were used by the Project Team to reach these objectives. More specifically, the data collection activities in which the Project Team was engaged are described here.

Chapter 2: Problem definition

Problem definition (Task 1) plays a pivotal role in understanding the key problems, their underlying causes (drivers) and consequences. In order to define the problem,

1. First, the Project Team conceptualised the problem tree following the guidance set in Tool #14 of the Better Regulations Toolbox on how to analyse problems and draft a preliminary intervention logic to be tested.
2. Second, the Project Team presented the policy objectives, specifying what are the general and specific objectives, what specific objectives address the problem drivers, and what objectives are consistent with other EU policies and legislation.
3. Third, the Project Team presented the rationale for EU action and addressed whether the legal basis and the subsidiarity principles are respected.

Chapter 3: Identification of ICT product categories and risk profiles

The identification of ICT product categories and risk profiles (Task 2) is a key step in the development of future policy options by providing a framework to classify ICT products and to determine the level of risks associated:

1. First, the Project Team provided a definition for ICT Products as well as a categorisation of ICT Products into six categories.
2. Secondly, the Project Team presented the different risk profiles determined for the ICT products categories across the sectors selected for the Study, and drew conclusions from this exercise.

[7] https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en

Chapter 4: Selection of cybersecurity requirements

Closely linked to Task 2, the selection of cybersecurity requirements (occurred under Task 3) provides a baseline, composed of a lifecycle, of Essential Requirements and security requirements as well as conformity assessment activities which can be used to ensure the cybersecurity of ICT products:

1. First, the Project Team defined a generic life cycle model for ICT products and identified generic stakeholders involved in the lifecycle.
2. Secondly, the Project Team presented the Essential Requirements identified and their corresponding security requirements.
3. Lastly, the Project Team provided a list of assessment activities to be used in the evaluation of the conformity of ICT Products, on the basis of their risk profiles.

Chapter 5: Identification of policy options

Identification of policy options (Task 4) elaborates on the different policy options based on the gap analysis of existing legislation (Task 1) and identified categories of ICT products and corresponding risk profiles (Task 2) and the identification of security requirements (Task 3):

1. First, the Project Team mapped the NLF against the preliminary policy options.
2. Second, the Project Team presented the analysis of the policy options, namely Baseline, Voluntary measures, Horizontal legislation, Sector-specific legislation and the Mixed approach.
3. Third, the Project Team mapped the policy options against problem drivers and policy objectives.

Chapter 6: Analysis of the possible impacts

Analysis of the possible impacts (Task 5) assesses the possible impacts of the selected policy options provided from Task 4:

1. First, the Project Team presented the analysis of the possible impacts on the assessment criteria of Effectiveness and social impacts, Efficiency and economic impacts, Coherence, Fundamental rights, EU added value, Environmental impact.
2. Second, the Project Team presented a comparison of the policy options taking into account the main assessment criteria.

Chapter 7: Conclusions and recommendations for EU Action

Finally, the last Chapter of the report summarises the main findings of the study and provides recommendations for the next steps European Institutions could follow to enhance the security of ICT Products.

1 Scope and methodology

This Chapter presents the scope and the overall objectives (section 1.1) of the "Study on the need of cybersecurity requirements for ICT products", as well as the data collection methods (section 1.2) used to gather supporting evidences in the context of the different tasks.

1.1 Scope and objectives

The study supports the work of the European Commission by exploring the current state of cybersecurity for ICT products. The study provides an in-depth analysis of the current regulatory framework with regard to cybersecurity requirements for ICT products, identifying the reasons underpinning the lack of adequate security to cyberthreats of these products. It also selects and explores the possible policy options for an appropriate intervention by the policy makers to address the gaps in the regulatory environment covering ICT products.

The results of this study inform the European Commission on the impacts that a policy intervention can have on the economy and on society as a whole. It will benefit from research, analysis, and stakeholder consultation in line with the European Commission's Better Regulation Guidelines and Toolbox.

The study is driven by six core objectives:

1. **Definition of the problem.** The study provides an overview of the current legislative framework for ICT products both at European and national level, by identifying the main problems, drivers, and consequences linked to cybersecurity requirements for ICT products. Particularly, the study builds on:
    - A list of existing and upcoming EU and national legislation and initiatives,
    - An analysis of the current gaps in terms of cybersecurity requirements,
    - A conceptual definition of the main problem.
2. **Categorisation of ICT products and their risk profiles.** The study defines an appropriate terminology for ICT products as a first step towards a common understanding of relevant cybersecurity scenarios. It undertakes a risk assessment to identify the risk profiles inherent to each category of ICT products. The risk assessment establishes how the identified categories of ICT products differ based on their use in specific sectors.
3. **Identification and recommendation of a set of essential cybersecurity requirements.** The study provides a set of essential cybersecurity requirements specific to each risk profile. These requirements consider the whole lifecycle of an ICT product. For example, the study examines the potential impact of first-party conformity assessment carried out by an ICT manufacturer in view of the low level of vulnerabilities associated with ICT products.
4. **Proposition of a set of policy options.** On the basis of the gap analysis of existing EU and national legislation, and the identified categories of ICT products and corresponding risk profiles, the study defines a baseline scenario that represents the situation 'as if' no action at EU level will be taken as well as elaborates a set of policy options, namely:
    - Policy Option 1: Voluntary measures for the industry;
    - Policy Option 2: Horizontal legislation applicable to all categories and risk profiles of ICT products (essential cybersecurity requirements);

  - Policy Option 3: Legislation applicable only to specific ICT product categories or risk profiles (sector-specific or intended use); and
  - Policy Option 4: Mixed approach: implementation of voluntary measures and regulatory approach based on specific categories and risk profiles of ICT products.

5. **Assessment of the impact of each policy option.** The study estimates the likelihood and the magnitude of the impacts (i.e. economic, social, and environmental) for each policy option. Once both positive and negative impacts are assessed, the study develops a cost-benefit analysis (CBA) for each of the policy options previously identified. The study analyses the benefits and the costs stemming from the different options not only in relation to all the relevant economic operators but also to national authorities and end-users of ICT products.
6. **Formulation of conclusions and recommendations** on the optimal way forward based on the assessment of impacts of the identified policy options.

1.2 Methodological approach

The impact assessment builds on a variety of data collection methods that allowed the Project Team to develop a comprehensive assessment based on the views of several stakeholders' groups (see stakeholder categories in Table 2) across the EU Single Market. Particularly, the following research instruments have been used in the context of the study:

- **Desk research** on relevant documents, among which, EU laws, EU publications, positioning papers both of consumer and industry associations as well as academic publications. A complete overview of all the secondary sources used by the Project Team is available in Annex I – List of secondary sources. The desk research was instrumental to inform the problem definition and baseline, the different policy options, and assessment of their expected social and economic impacts.
- **Semi-structured interviews** targeting stakeholders working within EU Institutions and Agencies as well as ICT industry experts and relevant EU and national associations. The interviews helped the Project Team to explore the issues identified in the desk research in ICT in further depth, acquiring expert information and insights from a range of players in the ICT ecosystem.
- **Focus groups** targeting several stakeholders' categories aimed to discuss specific issues relating to ICT product cybersecurity and to complement the information and findings stemming from the other data collection activities. Particularly, the focus group meetings sought to gather stakeholders' views and needs regarding certain issues related to the cybersecurity of ICT products across the EU.
- **Workshops** targeting all stakeholders' categories were instrumental to engage a broader audience in an interactive discussion on a broad variety of questions related to the different tasks of the study. The Project Team performed three workshops focusing on homogeneous groups of study questions (i.e. (i) problem definition; (ii) product categories and essential cybersecurity requirements and; (iii) identification and assessment of policy options) with the aim of gathering feedback on the final conclusions resulting from the data collection activities of the different tasks.
- **Delphi panel** targeting stakeholders that have been previously involved in the stakeholder consultation activities. The Delphi Panel helped the Project Team to collect anonymous but granular evidence from a reduced audience of high-level experts on the impact of the policy options.

- **Targeted consultation** targeting all the stakeholders that have been previously contacted by the Project Team. The targeted consultation has been instrumental to collect stakeholders' feedback on the preliminary results of the study, enriching them with additional perspectives and evidences.

All the stakeholder engagement activities involving a direct discussion with relevant stakeholders (i.e. interviews, focus groups, workshops) have been performed using videoconferencing tools to ensure continuity of project delivery during the COVID-19 pandemic.

Table 1 presents an overview of the different data collection activities by objective of the study as described in section 1.1. All the objectives have been assessed by at least four different data collection activities.

Table 1 Data collection activities by study objective

Data collection activity	Task 1 Problem definition	Task 2 Product categories and associated risks	Task 3 Cybersecurity requirements	Task 4 Identification of policy options	Task 5 Assessment of policy options
Desk research	✓	✓	✓	✓	✓
Semi-structured interviews	✓	✓	✓	✓	
Focus groups	✓	✓	✓		
Workshops	✓	✓	✓	✓	✓
Delphi panel					✓
Targeted consultation	✓	✓	✓	✓	✓

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

During the stakeholder engagement activities, the Project Team targeted several stakeholder groups as described in Table 2.

Table 2 Stakeholders groups categories

Category	Description
Category 1 – European Institutions and Agencies	Policy-Makers at the EU level (i.e. European Commission, other EU institutions and Agencies)
Category 2 – National competent authorities	Member State competent authorities (ministries or governmental bodies) with expertise in the implementation of EU legislation in the areas of product safety and cybersecurity (e.g. GPSD, RED, Cybersecurity Act); national accreditation bodies; conformity assessment bodies, national standardisation bodies and; market surveillance authorities having responsibilities for the enforcement of the requirements of EU product safety and cybersecurity laws
Category 3 – ICT industry	ICT product developers and engineers; ICT device manufacturers and; ICT maintenance and repair services
Category 4 – Academic experts	University professors; PhD students and; independent consultants specialised in the ICT industry
Category 5 – Professional associations	Representatives of users in professional sectors that critically rely on ICT and that make use of sector-specific ICT products or services (e.g. banking, transport)
Category 6 – Consumer associations	Representatives of consumer organisations.
Category 7 – Other	Representatives of other stakeholder groups not included in the previous categories

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

1.2.1 Desk research strategy

The objective of the desk research activities is to analyse the existing evidence, collecting the state-of-art around the need of cybersecurity requirement for ICT products in the EU. Hence, the Project Team performed an extensive desk research exercise to feed each task, gathering all the information available from several type of sources.

The study relies on the analysis of the EU legal and policy documents such as:

- *EU legislation.* The Project Team analysed several pieces of legislation in the field cybersecurity (e.g. Cybersecurity Act[8]) and others included in the NLF (e.g. Machinery Directive[9], General Product Safety Directive[10]).
- *ENISA studies and reports.* ENISA has published several reports highlighting the role of cybersecurity as source of competitive advantage for businesses and key pillar to ensure consumers' trust in digital technologies.

[8] 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 on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, 7 June 2019, Brussels.

[9] Directive (EU) 2006/42 of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, 9 June 2006, Brussels.

[10] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

- *European Commission Communications.* Recognising the geographical fragmentation of the EU internal market, the European Commission called in several occasions for actions to foster a more integrated single market for cybersecurity products and services.
- *European Council Conclusions.* The European Council has called for actions to fight against cyber and cyber-enabled illegal and malicious activities as well as to setup a strong cybersecurity capacity.
- *Council of the EU Conclusions.* The Council stressed the need to strengthen digital trust and security, which includes both ICT products and services, and to minimise fragmentation of the Single Market, aiming at an efficient, transparent and coherent European framework.
- *European Parliament Resolutions.* The European Parliament called the European Commission to put forward a proposal for a horizontal piece of legislation introducing cybersecurity requirements for ICT products .

Moreover, the study also builds on the analysis of relevant *academic publications*, *positioning papers of consumer and industry associations*, *reports from key ICT stakeholders* as well as *grey literature*. Along with the EU legal and policy documents, this documentation represented the starting point to define study issues that have been further assessed throughout the stakeholder consultation activities. A full list of the references used in the desk research activities is available in Annex I – List of secondary sources.

1.2.2 Semi-structured interviews' strategy

The aim of the semi-structured interviews was to gather data and information from various stakeholders' groups, collecting feedback on study issues identified during the desk research while obtaining access to new insights on the cybersecurity of ICT products across the EU. The Project Team performed **52 semi-structured interviews** with different stakeholders. The interviews lasted between 45 minutes and one hour and a half, depending on the topic under discussion and the relevance for more than one task. Table 3 provides an overview on the number of interviews performed in the context of each objective of the study.

Table 3 Number of interviews by study objective

Data collection activity	Task 1 **Problem definition**	Task 2 **Product categories and associated risks**	Task 3 **Cybersecurity requirements**	Task 4 **Identification of policy options**	Task 5 **Assessment of policy options**
Interview	7	22	4	19	-

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

In order to maximise the response rate and collect extensive feedback from key stakeholders, the Project Team has performed a step-by-step approach to conduct the interviews:

- *Selection of relevant stakeholders.* In the context of each task and following the guidelines defined by the First Inception Report (D1), the Project Team provided DG CNECT with a list of stakeholders to be interviewed. The list was composed of a priority sub-list as well as a reserve list to ensure that, in case one or more stakeholders declined the invitation or proved to be unresponsive, back-ups would guarantee the performance of the expected number of interviews.

- *Drafting of the interview guides*. Following the information contained in the ToR and the preliminary desk research activities, the Project Team developed interview guides based on the identification of relevant questions and topics to be discussed with the selected stakeholders.
- *Conducting the interview.* Once they have accepted the invitation, the targeted stakeholders were provided with the interview guide in advance of the interview so they could prepare their answers. In-depth interviews were conducted remotely following the questions included in the interview guides and asking additional clarification on arising matters when needed. The responses were typed during interviews and the minutes subsequently saved.
- *Finalisation of the interviews.* After conducting the interviews, the minutes were sent to the respective interviewees to receive the final validation. The Project Team performed a subsequent analysis of the filled-in interview guides.

Table 4 below presents the division of interviews by stakeholder group.

Table 4 Number of interviews by stakeholder group

Data collection activity	European institutions and agencies	National competent authorities	ICT industry	Academic experts	Professional associations	Consumer associations	Other
Interview	9	10	8	5	16	3	1

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

In addition to the semi-structured interviews, the Project Team performed a survey addressed to national competent authorities of EU Member States. Having received the approval from DG CNECT, the Project Team sent the questionnaire requesting written answer to a set of questions focused on national legislation and initiatives on ICT product cybersecurity as well as on general issues related to the problem definition. The Project Team received 12 replies in a two-weeks period.

1.2.3 Focus groups strategy

The aim of the focus group meetings was to collect stakeholder views by means of interactive discussion within and across stakeholder groups. The focus groups were instrumental to gather stakeholders' feedback on the preliminary findings of each task. The Project Team performed **9 focus groups** with different stakeholders. Table 5 provides an overview on the number of focus groups performed in the context of each study objective.

Table 5 Number of focus groups by study objective

Data collection activity	Problem definition	Product categories and associated risks	Cybersecurity requirements	Identification of policy options	Assessment of policy options
Focus group	2	4	3	-	-

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

In order to maximise the response rate and collect extensive feedback from key stakeholders, the Project Team has performed a step-by-step approach to the focus groups.

The Project Team provided DG CNECT with a list of stakeholders to invite to the focus groups. As in case of the interviews, the list was composed of a priority sub-list as well as a reserve list to ensure that, in case one or more stakeholders declined the invitation or proved to be unresponsive, back-ups would guarantee the performance of the expected number of participants to the meetings. The aim was to guarantee five to 10 participants per focus group meeting.

Ahead of the focus group, participants were provided with an explanation of the context of the study as well as draft agendas. Each focus groups lasted approximately two hours. During the focus groups, the Project Team presented the key findings resulting from the other data collection activities to the meeting participants. The interactive part consisted in an open debate moderated by the Project Team. In some occasions, the Project Team fostered the interactions among stakeholders through the use of design thinking tools (e.g. Mural).

1.2.4 Workshops strategy

The aim of the workshops was to collect the feedbacks on the preliminary results of the different tasks from a large audience of stakeholders across all stakeholders' groups. Particularly, the study entailed the organisation and performance of three workshops. Particularly:

- *Workshop 1* aimed to validate the findings of the Second Interim Report (D2), mainly presenting to relevant stakeholders the mapping of the existing EU and national legislation, and upcoming initiatives, the legislative gap analysis and the problem tree (Task 1);
- *Workshop 2* sought to share the findings related to the technical aspects of the project, focusing on the ICT products categories, risks profiles (Task 2) and present a generic life cycle model for ICT products, to present the identified cybersecurity requirements, and the corresponding conformity assessment procedures (Task 3);
- *Workshop 3* aimed to share and validate the different policy options developed in the context of Task 4 as well as gathering qualitative feedback that could be instrumental to the analysis of the impacts (Task 5).

Table 6 illustrates a schematic summary of the topics discussed during the workshops as well as the total number of stakeholders that participated to each workshop (**214 participants in total**).

Table 6 Workshops' number of participants

Workshop	Total number
Workshop 1 – Problem definition	42
Workshop 2 – Essential cybersecurity requirements	46
Workshop 3 – Policy options	126

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

The Project Team organised the three workshops following five main steps as follows:

- *Selection of relevant stakeholders*. In the context of each task and following the guidelines defined by the First Inception Report (D1), the Project Team provided DG CNECT with a list of stakeholders to be invited to the workshops.
- *Preparing the logistics.* Following an agreement with DG CNECT, the Project Team opted for the use of WebEx as videoconferencing solution to host the workshops. By enabling the use of polling during the workshop, WebEx represented a useful tool to steer the discussion on some key study issues.
- *Scoping the workshops.* Ahead of the workshops, the Project Team presented DG CNECT with the agenda of the workshop as well as the main materials to be shared for discussion. Draft agendas were developed

and refined based on the information gathered during the research. Following the feedback received by DG CNECT, the Project Team refined the agenda and the material.

- *Running the virtual workshops*. The Project Team presented the material that had been previously approved by DG CNECT while moderating the discussion thanks to the use of polling questions to obtain stakeholders' opinions on the preliminary results.
- *Producing the summary reports.* The Project Team produced three virtual workshops summary reports summarising the main discussion points and potentially agreed outcomes against the discussion questions.

1.2.5 Delphi panel strategy

The objective of the Delphi panel was to collect qualitative evidence from experts. In contrast with other data collection tools, the Delphi panel aimed to collect granular evidence from a reduced and targeted audience of high-level experts from the field of ICT product cybersecurity. The research team has conducted an online Delphi panel between 16-22 February 2021. The team invited to participate in the panel stakeholders who already participated in the third workshop on the identification of the policy options that took place online on 4 February 2021. This strategy ensured that stakeholders responding to the panel are the most familiar with the possible options and, therefore, were able to provide rich data on their possible impacts.

Out of a total of 34 responses received, the most came from National Competent Authorities (15), ICT Industry (9) and Academic experts (7). Table 7 breaks down the responses to the Delphi panel by stakeholder group.

Table 7 Number of stakeholders replying to Delphi panel by stakeholder group

Data collection activity	European institutions and agencies	National competent authorities	ICT industry	Academic experts	Professional associations	Consumer associations	Other
Delphi Panel	0	15	9	7	1	1	1

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

1.2.6 Targeted consultation strategy

An online targeted consultation was conducted as part of this study to allow a wider audience of experts, professionals and other relevant interested parties to express their views on current EU legislation and options for future EU legislation around cybersecurity requirements for ICT products. More specifically, the targeted consultation sought views on:

- Current issues around cybersecurity of ICT products and the appropriateness of legislation to address it (Problem definition);
- Cybersecurity issues as per categories of ICT products and risk profiles;
- Proposed policy options for ICT Cybersecurity going forward; and
- The likely impacts of the proposed policy options.

The online targeted consultation was launched in April 2021 and ran for a period of 6 weeks. It closed on 21 May 2021. As this was a targeted consultation, the Project Team identified the potential respondents from relevant institutions and organisations in the fields of ICT and cybersecurity policy based on the contacts database agreed with DG CNECT during the course of the study.

A 'snowball sampling' method was also used whereby the invited stakeholders were encouraged to share the link to the targeted consultation within their professional networks.

A total of 88 responses were received to the targeted consultation. More than two-thirds (71%) of the respondents either represented National competent authorities (NCAs) or the ICT industry. Responses from academic experts and representatives of professional users represent 17% of the total response. A few consumer associations, the key EU-level ones, also contributed their response to this survey. Two responses were received from representatives of EU Institutions.

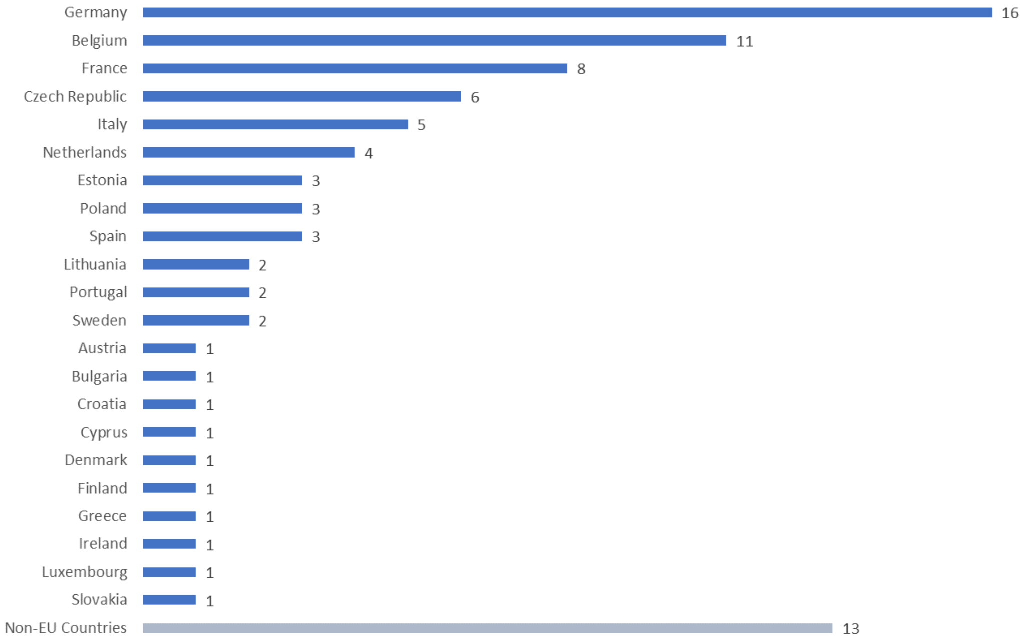
Table 8 Stakeholder types in the sample

Stakeholder type	No. of responses	% response
European Institutions	2	2%
National competent authorities	36	41%
ICT industry players	26	30%
Academic experts	8	9%
Professional users	7	8%
Consumer associations	5	6%
Other	4	4%
Total	**88**	**100%**

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

There was a total of 16 responses received from Germany, followed by 11 from Belgium, and 8 from France while 13 came from respondents in non-EU countries. There were on average very few responses from the remaining Member States and none from the following Member States: Hungary, Latvia, Malta, Romania, Slovenia. It is for these reasons that the survey responses have not been analysed by country.

Table 9 Overview of responses by country



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

1.2.7 Limitations on the data collection activities

As outlined in the previous paragraphs, the study relied upon several data collection methods (i.e. desk research, interviews, focus groups, workshops, ad hoc surveys, Delphi panel, and targeted consultation) that allowed the Project Team to gather important evidences from a large sample of stakeholders (over 270 individuals) across seven categories of stakeholder groups, representing relevant ICT sectors and EU Member States. The different research tools used in the context of the study helped the Project Team to collect heterogeneous views on key study issues, allowing us to analyse problems and solutions from different perspectives over a period of nine months.

The Project Team performed extensive research activities that allowed the compilation of important findings in the field of the cybersecurity of ICT products. In this regard, the continuous interaction with a great array of stakeholders represented an added value to the study. The findings of each task have been challenged by all stakeholder categories in several occasions, allowing the Project Team to account for the complexity inherent to the subject under analysis. Nevertheless, the Project Team deems important to highlight some margin for improvements that upcoming research on the subject matter should take into account:

- **Scarcity of quantitative data.** The desk research activities and the evidences collected through stakeholders' consultations allowed the Project Team to benefit from relevant statistics and quantitative data. Particularly, the study gathered primary data sources through several consultation methods such as interviews, focus groups, and workshops. These evidences have been used to complement the data publicly available online (e.g. Eurostat databases), strengthening the analysis across all tasks. However, the study could not rely on the analysis of public available structured databases on cybersecurity for ICT products. Some of the reasons behind the absence of quantitative data can be twofold: (i) the broad scope of the study that did not allow the Project Team to focus on any specific type of product and/or product category during the problem definition phase, and (ii) the scarcity of publicly available database on cybersecurity for ICT products;

- **Difficult to identify and assess cost.** While the stakeholders where able to provide rich qualitative data, the identification of costs was more difficult to obtain in large part due to the forward-looking nature of the topic and the lack of previous similar legislation to use as a benchmark. In order to help stakeholders identify costs, the Project Team used calculations of costs from previous relevant results from the Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment[11], a study on Evidencing the Cost of the UK Government's Proposed Regulatory Interventions for Consumer IoT[12], and interviews conducted as part of this study and asked stakeholders to consider whether the costs in the context of cybersecurity for ICT products would be lower, similar or higher. Consequently, the results on costs should be treated as indicative.
- **Limited statistical representativeness.** The targeted consultation complemented the original findings, providing useful insights on key study questions and allowing the Project Team to collect additional views from relevant stakeholders. This helped the Project Team to provide a more granular analysis on the main issues identified during the data collection activities. The study could rely on 88 responses submitted by different stakeholder groups. While national competent authorities and ICT industry accounted for the majority of the responses, academic experts and consumer associations have also participated to the targeted consultation, providing complementary feedback that strengthened the validity of the findings. On the other hand, the sample has a limited representativeness of European or national populations, population sub-groups or stakeholder types as they employ non-probability sampling. Therefore, from a statistical perspective, responses cannot be extrapolated to a given population, but are only representative of those who responded to the survey.

[11] The study is available at: https://ec.europa.eu/docsroom/documents/40763

[12] The study is available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf

2 Problem definition

This section presents the background and policy context related to the cybersecurity of Information and Communication Technology (ICT) products for the study, a gap analysis on a set of 37 pieces of EU legislation part of the NLF or applying directly or indirectly to the cybersecurity of ICT products (e.g. eIDAS Regulation, General Data Protection Regulation) and an analysis of legislation targeting ICT product cybersecurity at the Member States level. Moreover, this section includes the problem tree, identifying the main problems, their drivers and potential consequences.

The study provides an overview of policy background underpinning ICT product cybersecurity, from the first Cybersecurity Strategy of the European Union to the latest European Commission strategy, Shaping Europe's Digital Future. Furthermore, the study presents a list of EU legislation with the objective to describe their strengths and limits regarding the cybersecurity of ICT products. The Project Team has also included a section on adopted and forthcoming national legislation in order to provide an overview on ICT product cybersecurity at Member State level.

The gap analysis allows the Project Team to provide some key conclusions concerning the overall fitness of the EU legislative framework concerning the cybersecurity of ICT products. Particularly, the Project Team has found that (i) the current EU legislative framework does not cover all the security objectives set out in Art. 51 of the Cybersecurity Act; (ii) legislation related to the NLF does not address fully the cybersecurity requirements for ICT products; (iii) the granularity of some of the requirements identified in the legislation does not guarantee the fulfilment of the security objectives and; (iv) some cybersecurity requirements addressed to service operators apply indirectly to ICT products used to operate the service.

The baseline for this analysis was the Cybersecurity Act, this being one of the most recent, up-to-date, and relevant piece of EU legislation covering cybersecurity for ICT products at broad spectrum. It is used here as a preliminary point of reference for the legislative gap analysis but does not imply any set orientations on the policy options that will be detailed in Task 4, nor on the need of certification for ICT products at that stage.

Moreover, this chapter presents an in-depth analysis of the two main problems identified during the data collection activities, namely the lack of secure ICT products across the EU (i.e. Problem 1) and the insufficient understanding among users (e.g. citizens and companies) of the level of cybersecurity for ICT products (i.e. Problem 2). Following Tool #14 of the Better Regulation Toolbox, the Project Team describes their main drivers as well as possible consequences.

Lastly, the chapter presents the general and specific policy objectives resulting from the problem drivers and provides the rationale for EU action, assessing whether a possible EU intervention would have legal basis and evaluation whether the principle of subsidiarity has been respected.

2.1 Background and policy context

In order to properly address the policy issues related to the cybersecurity of ICT products, it is necessary to consider the specific market dynamics affecting these products. In this regard, section 2.1.1 describes the market dynamics by looking at two market failures related to ICT products, namely the presence of information asymmetries within the market and the existence of negative externalities. These market failures need to be considered when conducting a study aimed at increasing the cybersecurity of the ICT products.

2.1.1 Analysis of ICT products market

Many ICT products have software embedded and are able to connect to networks. Besides the very recent attention from policy makers to these products, it is important to mention that while in some sectors such as aeronautics, manufacturers have been ahead of regulation taking into account cybersecurity[13] in their production processes, the software industry has, for instance, strongly opposed for fifty years liability for its products, as the car industry did for the first seventy years of its existence. This approach is generated by bad economic incentives that, according to some researchers, can be as detrimental for security as bad technical design[14]. Such an approach from the software industry has its own rationality. In a market in which network economics apply, exploiting 'first-mover' advantage requires being first to market even if the product is not perfect ("*we'll ship it on Tuesday and get it right by version 3.0*")[15]. However, it is clear that this approach values cost-effectiveness, usability, and time market over security. Indeed, using security by design guidelines and updating software rise costs, increase time to market and make products less-user friendly with negative effects on the product demand. Therefore, a rational behaviour from a company conflicts with the optimal level of security. This misalignment of incentives while in competitive market in general does not exist, in market with network economics[16] is becoming the norm.

An additional case of misaligned incentives occurs in more mature markets and in the economic literature is mentioned as the "*Durable goods monopoly problem*". When a software designer has reached dominance in a market, it is difficult to convince his own customers to buy a new version of the product when it is made available. In other words, the dominant firm must compete with its own installed base. The economic literature suggests different ways in which the dominant operator can approach this issue[17]. First, the dominant firm can rent or lease its product. This is what software companies do by offering their products as a service to keep their customers with the most recent version of their software. Second, the company can produce fewer durable goods, i.e., use "planned obsolescence" to avoid reducing its price in the future, but also stopping updating software to incentivize customers to buy new products. This creates the incentive to shorten the commercial life of the product, affecting its own security reducing the length of the warrantee or the delivery of security updates [18].

Information asymmetries and negative externalities

Even if the alignment of incentives is correct, the market could fail in delivering optimal levels of security given to information asymmetries and negative externalities. Examining the ICT Products market, market failures are generated from one side by information asymmetries: the customer does not have a clear and neutral information

[13] OECD (2019), Role and Responsibility of Actors for Digital Security

[14] Anderson and Moore (2006), Information Security Economics – and Beyond

[15] Anderson (2001), Why information Security is Hard – An Economic Perspective, Paper prepared for 17th Annual Computer Security Applications Conference (ACSAC01), EEE Computer Society, December

[16] Market with network economics are characterized by: 1) high fixed costs and low marginal costs; 2) network externalities on the demand side; 3) path dependency ;4) customers lock-in. Therefore, the outcome of these market is quite often "the winner takes all". See on this Varian and Shapiro (1999), Information Rules, Harvard Business School Press.

[17] Carlton and Perloff (1994), Modern Industrial Organization, p.654

[18] OECD (2021a), Understanding the digital security of Products-An in-depth analysis, forthcoming.

on the product level of security; from the other side by negative externalities: software producers are not accountable for the damages created by the exploitation of vulnerabilities in their products.

Information asymmetries

The theory of perfect competition assumes that economic agents have complete and perfect information about all the variables that affect their transactions. However, in practice this situation occurs very rarely since quite often an imbalance of information between buyers and sellers exists. This situation of imbalance of power in the transactions, in contract theory and economics is called information asymmetry and can generate market failure. This theory was developed by George Akerlof, Michael Spence and Joseph Stiglitz. These authors all shared the Nobel Prize in economics in 2001 for their contribution to this theory. Asymmetric information theory indicates that sellers may have more information than buyers and that low-quality and high-quality products can command the same price, since a lack of information from the buyer side does exist. In particular, Akerlof looking at the car secondary market, in a paper of 1970 entitled "The Market for lemons: Quality uncertainty and the Market Mechanism ", argues that, since car buyers have different information than car sellers, they are unable to distinguish between "lemons"-i.e., Poor quality cars- from a good car. Therefore, while the seller of the lower quality car is aware of the lower quality of his product but does not bear any consequences for it (**moral hazard**), at the end of the transactions, only lower quality cars are sold in the market (**adverse selection**) since seller of high-quality cars cannot differentiate their products.

Information asymmetries characterize markets for ICT products containing software. Indeed, while consumers are able to understand usability and price of a product, they are unable to assess the level of security of it. This can generate adverse selection: since customers are unable to distinguish more secure products from less secure products, offering more secure products by developers will not be rewarded since customers will not be willing to pay for it.

Externalities

Externalities are defined as "*costs or benefits of market transactions to third parties, other than buyers or the sellers of a good or services, not reflected in prices*"[19]. The damage caused by industrial pollution to people and their property is considered a typical example of negative externality, while the benefit given to the members of a network who join the network, a case of positive externality. In both cases, if the externality is not internalized with a tax in the first case or with an incentive in the second case, the result is a suboptimal market outcome. Cybersecurity is a case in point!

Worldwide spending[20] on cybersecurity in 2019 exceeded USD 124 Billion and has been forecasted to reach over USD 133 billion in 2022. At the same time, according to a report published jointly by the Centre for Strategic and International Studies and McAfee the cost of cybercrime worldwide in 2016 has been about USD 600 billion, or 8% of global GDP, rising from USD 500 billion estimated for 2014[21]. The cost of cybercrime is estimated as the cost of

[19] Hyman D, (1987), Public Finance, A Contemporary Application of Theory to Policy, The Dryden Press p.82-83

[20] For spending on cybersecurity here is meant the companies' expenditures in software and hardware in the following market segments: Application Security, Cloud Security, Data Security, Identity Access Management, infrastructure Protection, Integrated Risk Management, Network Security Equipment, Other Information Security Software, Security Services, Consumer Security Software. See Gartner (2018), Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, August. Available at: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[21] CSIS, McAfee (2018), Economic Impact of Cybercrime-No Slowing Down, February

the activities by criminals gaining illicit access to a victim's computer or network. Using this definition, the elements of cybercrime cost identified include:

- The loss of intellectual property and business confidential information;
- Online fraud and financial crimes, often the result of stolen personally identifiable information (PII);
- Financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of performance reports for publicly traded companies;
- Opportunity costs, including disruption in production or services, and reduced trust for online activities. This includes the effect of ransomware, which involves both payments to redeem encrypted data if the victim choses to pay,[22] and, more importantly, serious disruptions to services and output, as well as costs related with the management of the ransomware (crisis costs, investigation and defence plan costs, rebuilding costs, etc.);
- The cost of securing networks, buying cyber insurance, and paying for recovery from cyberattacks;
- Reputational damage and liability risk for the hacked company and its brand, including temporary damage to stock value.

As far as investment in cybersecurity are concerned, the Gordon-Loeb model analyses the optimal investment level in information security[23]. The model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. More specifically, the model shows that it is generally not interesting to invest for amounts in information security higher than 37% of the predicted loss. In this case being the estimated loss about USD 600 billion, the optimal investment in information security should be about USD 222 billion far above the USD 124 billion spending in cybersecurity in 2019.

Such imbalance shows that let alone the market is unable to deliver appropriate quality and quantity of cybersecurity investment. In this respect, the cybersecurity market seems to be rather characterized by market failures associated with negative externalities, free riding, and public goods. Indeed, while markets in general are considered relatively efficient, in cybersecurity they are often deemed to fail. According to Ross Anderson[24], the security of the entire internet is affected by the security measures taken by all internet users. For this reason, cybersecurity is considered a public good. The security provided by a computer owner benefits other computer owners connected to the network, making it less likely that they will be attacked using the computer of the first owner. But, since computer owners are not liable for the damage caused when their computers are attacked, they do not exploit the benefits from increased security. In the case of botnets for instance, the social costs of the Distributed Denial of Service (DDoS) attacks are not suffered by the end-users of the compromised device, the manufacturers of the device and the internet service providers. Very often, the users do not know that their device has been used as part of the botnet and the device manufacturers do not bear any economic costs generated by the DDoS created using these devices. Therefore, they do not provide the proper level of security since they are not present with the right incentives [25].

[22] CSIS, McAfee (2018), Economic Impact of Cybercrime-No Slowing Down, February

[23] Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Trans. Inf. Syst. Secur, 5(4), p. 438–457

[24] Anderson, R. (2001), Why information Security is Hard – An Economic Perspective, Paper prepared for 17th Annual Computer Security Applications Conference (ACSAC01), IEEE Computer Society, December

[25] OECD (2021), "Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

Furthermore, cybersecurity information sharing is also characterized by market failure and free riding. In fact, the cost for firms to disclose their own vulnerabilities could be significant, for example in reputational terms, and the benefit of disclosing information are slow to arrive and benefit all firms equally (including competitors). As such, a firm optimal choice would be to avoid exposing itself while still enjoying the benefit deriving from some else's disclosure.

There are many reasons to explain this behaviour:

- **Financial market impacts**: Stock and credit markets may react negatively to security breach announcements, increasing the cost of capital to reporting firms for being now perceived to be riskier than previously thought;
- **Reputation or confidence effects**: Negative publicity may affect firm's reputation or brand, generating loss of confidence from consumers and giving competitors competitive advantages;
- **Litigation concerns**: When a firm reports a security breach, investors, customers may use the courts to seek recovery of damages. Furthermore, if there is a track record of breaches, plaintiff may claim a pattern of negligence against the firm;
- **Liability concerns**: Officials of a firm or organisation may be subject to sanctions if they do not comply with regulations that establish ad hoc standards for safeguarding customers and users' records;
- **Signal to attackers**: Admitting publicly the breach, may alert hackers that an organisation's cyber defence is weak and suggest further attacks;
- **Job security**: IT personnel may fear for their jobs after an incident and try to hide the breach from senior management[26].

Therefore, it is clear that the aforementioned market dynamics and market failures need to be taken into account to design policies aiming at increasing the cybersecurity of the ICT products. This should be done trying to create better incentives for all stakeholders to provide an acceptable level of security; to increase product transparency so consumers can make more Informed choices about product security and to internalize the externalities previously mentioned in the product 's value chain[27].

2.1.2 Policy context

In recent years, a variety of Information Communication Technology (ICT) products and especially connected devices have turned everything into something connected and smarter. Indeed, Smart Home, Smart Building, Smart Grid, Smart Factory, Connected Cars and Autonomous Shuttle are now becoming a reality. However, while creating numerous opportunities for the European economy and society, the digitalisation brings forward several new challenges. According to a recent study made by a cybersecurity technological provider[28], cyber threats increase year over year, as the popularity of emerging technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), big data, the large use of cloud computing, as well as the network connected smartphones, provide copious ways to compromise the security of an organisation. Therefore, considering the possible economic and social

[26] See on this Cashell et al. (2004) , The Economic Impact of Cyber-Attacks. CRS Report for Congress, April 1

[27] OECD (2021), "Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

[28] 2020 Cybersecurity Report, Check Point, 22 January 2020.

consequences of cyber-incidents and cyber-attacks, the cybersecurity for ICT products represents the foundation of a prosperous European Digital Single Market.

The need to drive the development of cybersecurity within the European Union appears to be even more paramount with the advent of the IoT. This is because a large number of decentralised devices, inherent to the nature of the IoT, increases drastically the attack surface[29]. Another reason is that connected devices can also lead to physical damages, as an incident concerning ICT products can have an impact on the whole system, leading to severe consequences in terms of disruption to economic and social activities in case such ICT product is interconnected with critical infrastructures (e.g. hospitals, power plants). In addition, the use of heterogeneous and fragmented technologies as well as the emergence of new market players with low cybersecurity maturity multiplies the probability of attacks happening on connected devices.

Since 2005, when the European Commission recognised that ICT products and services are a powerful driver of growth and highlighted the urgent need to build stakeholders' trust in technologies, the European Union has striven to enhance cybersecurity within the internal market[30]. Focusing on the last 10 years, particularly relevant for the development of cybersecurity at the EU level was the 2013 **Cybersecurity Strategy of the European Union**[31] aimed to streamline the policy response of Member States to address cyber threats and risks.

Regardless of the area or sector under analysis, a strong cybersecurity has to be made a priority for the smooth functioning of the Union in this digital era[32], as stressed in the **European Council Conclusion of 18 October 2018** recalling the 19 June 2017 Council conclusions[33]. At the EU level, there is a strong political commitment behind the creation of an ambitious cybersecurity strategy. This is clear from the **joint communication to the European Parliament and the Council of 2017**[34]. The political commitment is also supported by the Commission's proposal of a financing programme to foster digital capacities: the **new Digital Europe Programme** for the period 2021-2027[35]**.** The Digital Europe Programme with an initially proposed overall budget of EUR 8.2 billion with EUR 1.8 billion allocated for cybersecurity aims to ensure sufficient financing for the EU and its Member States for accelerating cooperation on prevention, detection, and responses to cyber-incidents and cyber-attacks across the EU[36].

[29] Following Techopedia, "the attack surface of a system is the complete set of vulnerabilities that exist within that system. It is a metaphor used for assessing security in a hardware and software system. The attack surface is not an actual surface, but it helps the individual to visualise where vulnerabilities are in a system." Information available at: https://www.techopedia.com/definition/33810/attack-surface.

[30] COM(2005) 229 final, Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions "I2010 – A European Information Society for growth and employment", 1 June 2005, Brussels.

[31] Join(2013) 1 Final, Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, 7 February 2013, Brussels.

[32] European Council Meeting - Conclusions of 18 October 2018, Brussels.

[33] Council Conclusions on EU External Action on Counter-terrorism, 19 June 2017, Brussels.

[34] JOIN/2017/0450 final, Joint Communication to The European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13 September 2017, Brussels.

[35] SWD/2018/305 final - 2018/0227 (COD), Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027, 6 June 2018, Brussels.

[36] https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu82-billion-funding-2021-2027.

In its latest strategy, **Shaping Europe's Digital Future**[37], published in February 2020, the European Commission acknowledged once again that digital solutions such as IoT can enrich our lives in many ways but that the benefits arising from these technologies do not come without risks and costs. Citizens feel that they do not have control over their personal data and multiple cyberthreats jeopardise both European national critical infrastructures and wider security interests. For these reasons, key initiatives set by the Shaping Europe's Digital Future were the establishment of a joint Cybersecurity Unit, the revision of the NIS Directive, and giving a push to the single market for cybersecurity. In July 2020, during a speech delivered to the European Parliament, the European Commission President Ursula von der Leyen stated that cybersecurity currently represents a top priority for the EU[38]. Furthermore, following the **Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade**, the European Commission has also called for a more comprehensive approach to cybersecurity for connected products (e.g. duty of care for connected device manufacturers)[39].

As stressed in the **Council Conclusions on the cybersecurity of connected devices**[40], there is a need for horizontal legislation in the long term addressing all relevant aspects of the cybersecurity of ICT products, such as safety, liability, availability, integrity, and confidentiality, and in doing so make best use of cybersecurity certification. Such future legislation also requires relevant norms, standards or technical specifications, which keep into consideration the dynamic nature of cybersecurity (i.e. a secure product becoming insecure at a later stage when new vulnerabilities are discovered) and bring clarity over the attribution of damage along the supply chain in case of a failing in cybersecurity brings to a damage[41].

More recently, the European Parliament adopted a resolution on the **EU's Cybersecurity Strategy for the Digital Decade**[42]**,** calling the European Commission to explore the need for a horizontal piece of legislation mandating cybersecurity requirements for ICT products by 2023.

Numerous European strategies have over time addressed the need to increase the trust and cybersecurity in the Single Market, as reported by the Court of Auditors[43]. Despite this, the specific aspect of cybersecurity in ICT products has not been directly addressed by EU law. In fact, it appears that the existing European legislative framework might not be sufficient to tackle specifically the challenges linked to the security of connected products. An exception is the introduction of the Radio Equipment Directive (RED) [44] and its delegated acts, which could be seen as the first policy intervention directly targeting ICT products. Box 1 provides the state of play of the RED at

[37] European Commission (2020). Shaping Europe's Digital Future, European Commission, 19 February 2020.

[38] Information available at: https://ec.europa.eu/jrc/en/news/put-cybersecurity-at-centre-of-society#:~:text=In%20a%20speech%20to%20the,sides%20of%20the%20same%20coin.&text=That's%20because%20digitalisation%20indirectly%20exposes%20everyone's%20daily%20life%20to%20cyber%20threats.

[39] JOIN(2020) 18 final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020 Brussels

[40] Council Conclusions on the cybersecurity of connected devices, 2 December 2020, Brussels.

[41] European Court of Auditors, Briefing paper: challenges to effective cybersecurity policy, March 2019

[42] European Parliament (2021) The EU's Cybersecurity Strategy for the Digital Decade European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). P9_TA(2021)0286

[43] European Court of Auditors, Briefing paper: challenges to effective cybersecurity policy, March 2019.

[44] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, 25 May 2014, Brussels.

the time of writing this report. It should be noted that a future policy intervention should take into account the latest developments of the RED.

Box 1 Radio Equipment Directive (RED) – State of play as of February 2021

PURPOSE

The RED aligned the previous directive (1999/5/EC) with the NLF. The revision accounted for the need of improved market surveillance with particular focus on the traceability obligations of all the actors involved in the value chain (from manufacturers to distributors).

The RED defines the regulatory framework for the placement of radio equipment on the market. Particularly, Articles 3(1) and (2) of the RED sets out the essential requirements that radio equipment shall respect. Among these, some essential requirements concern the protection safety and health of people using radio equipment.

TIMING

The RED was published in the Official Journal of the European Union on 22 May 2014. The Directive entered into force on 11 June of the same year and became applicable in all Member States as of 13 June 2016.

SCOPE

Following Article 3(2) of the directive, the Commission shall adopt delegated acts clarifying which categories or classes of radio equipment will be concerned the essential requirements outlined in the same article. In this regard:

- Article 3(3)(g) was activated by means of Commission Delegated Regulation (EU) 2019/320 of 12 December 2018 supplementing of Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3)(g) of that Directive in order to ensure caller location in emergency communications from mobile devices.
- Articles 3(3)(d)(e) and (f) will be activated in 2021 for certain categories of equipment addressing the following issues:
    - radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
    - radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
    - radio equipment supports certain features ensuring protection from fraud.

The following sections provide an analysis on the existing European and national legislation in relation to cybersecurity for ICT products. For the purpose of this study, the Project Team has largely classified EU legislation as “horizontal”, where the provisions in relation to ICT products address several sectors of the economy (e.g. Cybersecurity Act), and “specific” where ICT products are addressed with regard to a specific sector (e.g. health).

2.1.3 European legislation

2.1.3.1 Existing legislation

There are currently several EU initiatives that address cybersecurity concerns in a horizontal manner. These initiatives provide an increased level of consumer protection and, thus, contribute to ensuring the continuity of services and the good functioning of the Union's economy and society. An example of horizontal legislation is the **Security of Network and Information Systems (NIS) Directive**[45], which seeks to build cybersecurity capabilities across the EU and mitigates growing threats to network and information systems used to provide essential services in key sectors (e.g. banking, energy, transport, healthcare and digital infrastructure).

The NIS Directive entered into force in 2016 and was transposed into national law by May 2018. Since then, the Directive has strengthened the European cybersecurity landscape, leading to the adoption and alignment of national cybersecurity strategies, and supporting cooperation and exchange of information among Member States, in particular, through a Cooperation Group and the CSIRT Network. The NIS Directive is currently under revision to further improve the resilience of the EU against cybersecurity risks and continue to foster swift and effective cooperation across the Union.

Another example of EU horizontal legislation in the cybersecurity domain is the **Cybersecurity Act**[46]**.** The Cybersecurity Act represented the first attempt made by the EU policymakers to solve the issue related to the existence of national certification schemes that are not recognised across the Digital Single Market. Indeed, the Cybersecurity Act introduces the possibility for business to certify that their ICT products, processes, and services fulfil EU cybersecurity standards. Once into place, this possibility will benefit significantly European companies that can have their certificates recognised across the Union. In addition, the Cybersecurity Act granted a permanent mandate to European Union Agency for Cybersecurity (ENISA), which can now better help the Member States with cybersecurity incidents and risks.

There are also numerous EU horizontal initiatives concerning liability and safety of products in the single market. For instance, the **RED**[47] establishes a European regulatory framework by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. Similarly, the **General Product Safety Directive**[48] **(GPSD)** ensures that only safe products are sold to consumers within the single market. Meanwhile, the **Product Liability Directive**[49]- a longstanding piece of legislation covering any product marketed in

[45] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 19 July 2016, Brussels.

[46] 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 on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, 7 June 2019, Brussels.

[47] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, 25 May 2014, Brussels.

[48] Directive (EC) 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety, 15 January 2002, Brussels.

[49] Directive (EEC) 85/374 of the Council of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, 25 July 1985, Brussels.

the EU - created a regime of strict liability for damage arising from defective products applicable in all Member States.

Furthermore, the **General Data Protection Regulation (GDPR)**[50], which came into effect in May 2018, contributes to creating more consistent protection for the privacy and security of citizens' personal data. In comparison to the former Data Protection Directive, the GDPR increased penalties for non-compliance that can amount to 4% of the violating company's global annual revenue. All organisations, from small businesses to large enterprises, regardless of their location, must now comply with GDPR requirements if they offer goods or services to EU citizens. As a result, the GDPR has a worldwide impact on data protection.

In addition to the horizontal legislation, sectoral EU interventions contribute to the European legislative framework for ICT products. The rationale behind EU sectoral legislation on security is to provide increased security standards for categories of products bearing a higher risk profile. The EU sectoral legislation includes, for instance, the **Machinery Directive**[51], which is the main European legislation regulating products of the mechanical engineering industries; and the **Medical Device Regulation**[52] that bounds manufacturers of medical devices to consider cybersecurity risks when placing products in the market. These pieces of legislation are just some of the many sectoral EU interventions that tackle issues and risks associated with specific categories of ICT products. Other examples include but are not limited to the **Civil Aviation Regulation**[53]**, the Competitiveness Terminal Equipment Directive**[54] **and the Consumer Right Directive**[55].

Table 10 below summarises the adopted horizontal and sectoral EU legislation in the scope of our study that touches upon the issue of cybersecurity for ICT products.

Table 10 Adopted EU legislation in relation to cybersecurity for ICT products

ID	Name	Category	Sector	Products in scope[56]
1	Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency	Sectoral	Aviation	Aircrafts, aircraft equipment
2	Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment	Horizontal	All	Terminal equipment, satellite earth station

[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 4.May 2016, Brussels.

[51] Directive (EU) 2006/42 of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, 9 June 2006, Brussels.

[52] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 5 April 2017, Brussels.

[53] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, 4 July 2018, Brussels.

[54] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, 21 June 2008, Brussels.

[55] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales»), 11 June 2005, Brussels.

[56] The Project Team aims to identify what kind of products (ICT products or not) might be impacted by the legislation. There might be no products is in scope of a given piece of legislation.

ID	Name	Category	Sector	Products in scope [56]
3	Unfair Commercial Practices Directive - Directive (EC) 2005/29	Horizontal	All	None
4	Cybersecurity Act - Regulation (EU) 2019/881	Horizontal	All	ICT products, products used in ICT services, ICT processes
5	Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code	Horizontal	All	Equipment's used in electronic communications and networks
6	Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union	Horizontal	All	Products used in non-personal data processing operations
7	General Data Protection Regulation - Regulation (EU) 2016/679	Horizontal	All	Products used in personal data processing operations
8	Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport	Sectoral	Transport	None
9	Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits	Sectoral	Energy & Electric	Electronic and electrical equipment (non-radio)
10	Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices	Sectoral	Health	In-vitro diagnostic devices and their accessories
11	Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices	Sectoral	Health	Medical devices, accessories and components
12	Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles	Sectoral	Transport	Motor vehicles of categories M and N and their trailers of category O, that are intended to be used on public roads
13	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	Horizontal	All	None
14	Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products	Horizontal	All	All
15	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment	Horizontal	All	Radio equipment
16	Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods	Horizontal	All	Goods with digital elements
17	Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products	Horizontal	All	Products that are subject to the Union harmonisation legislation
18	Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys	Sectoral	All	Toys
19	Directive 2010/35/EU of the European Parliament and of the Council of 16 June 2010 on transportable pressure equipment	Sectoral	All	Transportable pressure equipment

ID	Name	Category	Sector	Products in scope[56]
20	Directive 2013/29/EU of the European Parliament and of the Council of 12 June 2013 on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles	Sectoral	Pyrotechnic	Pyrotechnic articles and fireworks
21	Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft	Sectoral	Marine	Recreational crafts and personal watercraft
22	Directive 2014/28/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses	Sectoral	Explosive	Explosives for civil uses
23	Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments	Sectoral	All	Non-automatic weighing instruments
24	Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments	Sectoral	Construction	Measuring instruments
25	Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts	Sectoral	Construction	Lifts
26	Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment	Horizontal	All	Pressure equipment
27	Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment	Sectoral	Marine	Marine equipment
28	Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations	Horizontal	All	Cableway
29	Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment	Horizontal	All	Personal Protective Equipment (PPE)
30	Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels	Horizontal	All	Gas appliances
31	Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services - Directive (EU) 2019/770	Horizontal	All	Digital services, and ICT products with digital content
32	Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products	Horizontal	All	All
33	Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC	Horizontal	All	All
34	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market	Horizontal	All	Hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services
35	Directive on privacy and electronic communications - Directive (EC) 2002/58	Horizontal	All	Products used in personal data processing operations
36	Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety	Horizontal	All	All

ID	Name	Category	Sector	Products in scope[56]
37	Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC	Sectoral	Machinery	Machinery

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Overall, it appears that the European legislative landscape aiming to tackle cybersecurity incidents and threats and ensure the security of key areas of economic and social activity within the European Union, is broad and comprehensive, but it does not target ICT products specifically, as further described in the gap analysis (section 2.2). Ultimately, the concepts of 'safety' and 'cybersecurity' used in the current legislation are not detailed enough to protect consumers from the security breaches which come along with connected devices, as they do not directly concern ICT products.

Meanwhile, the Cybersecurity Act, which aims at creating a European framework for the certification of cybersecurity for ICT products and digital services, due to its voluntary nature, does not guarantee an automatic increase of the cybersecurity for ICT products placed on the internal market or a limitation of the fragmentation of the European cybersecurity framework. Indeed, while setting out key security objectives for ICT products that European cybersecurity certification schemes shall aim to address, the Cybersecurity Act did not make the adoption of such schemes for companies compulsory.

2.1.3.2 Upcoming legislation

New legislation was adopted and other are currently under discussion in the political agenda at the EU level. The Commission started to review the existing legislation at the end of the 90's, concluding that aspects related to the notification process, the conformity assessment procedures, CE marking[57] and market surveillance had to be updated. The review of the regulatory framework led to the **NLF[58]** , which was adopted on 9 July 2008 to **improve market surveillance rules while enhancing the quality of the conformity assessment.** The package of measures consists of:

- Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products [59];
- Decision 768/2008 on a common framework for the marketing of products[60];

[57] Products with the CE marking meet high safety, health, and environmental protection requirements, and can be traded in the EEA without restrictions. For further information, please refer to: https://ec.europa.eu/growth/single-market/ce-marking_en

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

[59] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, 13 August 2008, Brussels.

[60] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, 13 August 2008, Brussels.

- Regulation (EC) 764/2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State[61].

As a consequence of the introduction of the NLF, several directives and regulations were aligned with its reference provisions, such as RED; Low Voltage - Directive 2014/35/EU, Pressure equipment - Directive 2014/68/EU, and Marine Equipment - Directive 2014/90/EU, among many others.

In addition to the legislation affected or aligned to the NLF, the European Commission is drafting two relevant proposals regarding ICT products cybersecurity: The **Regulation on AI requirements** and the **Regulation on Digital Operational Resilience for the Financial Sectors** (DORA). DORA[62], published on 24 September 2020, represents a first European-level legislative initiative aiming to introduce a harmonised and comprehensive framework for European financial institutions. DORA will enhance and streamline ICT risk management, harmonise the reporting of ICT-related incident, improve digital operational resilience testing and increase awareness of cyber risks and ICT incidents. When officially adopted, DORA will also bring critical ICT third-party service providers (e.g. cloud computing) under the supervision of the European competent authorities.

Concerning the upcoming Regulation on AI requirements, the Commission presented the '**White Paper on Artificial Intelligence – A European approach to excellence and trust**'[63] in February 2020. The White Paper represented the first step of the legislative process for a comprehensive regulation of Artificial Intelligence, which will both promote the uptake of AI and address all risks associated with emerging technologies (e.g. violation of fundamental rights including personal data and privacy protection and non-discrimination). In April 2021, the European Commission published the proposal for a regulation of laying down harmonised rules on AI[64]. This proposal represents an attempt for an EU regulatory framework on AI, defining obligations for several actors across the value chain and operating in different sectors of the economy. Another objective of the regulation would be to foster the development of AI technology within the Single Market.

ICT product cybersecurity is also considered into the **revision** of different EU piece of legislations, such as the proposal for the revision of the **eIDAS Regulation - Regulation (EU) 910/2014**[65]; the proposal for the revision of the **Machinery Directive - Directive (EC) 2006/42**[66]; and the **General Product Safety Directive – Directive (EC) 2001/95** expected in Q2 2021. The revision of the eIDAS regulation considered both the demand for secure online transactions and the evolving cyber risks as drivers for innovation through AI and IoT in digital identity solutions[67]. The proposal introduced articles on the certification of European digital identity wallets as well as electronic

[61] Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC, 13 August 2008, Brussels.

[62] COM(2020) 595 final, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24 September 2020, Brussels.

[63] COM(2020) 65 final, White Paper on Artificial Intelligence: a European approach to excellence and trust, 19 February 2020, Brussels.

[64] European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts. COM(2021) 206 final. 2021/0106(COD). Brussels, 21.4.2021.

[65] European Commission (2021). Proposal for a Regulation of The European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. COM(2021) 281 final 2021/0136 (COD). Brussels, 3.6.2021

[66] European Commission (2021). Proposal for a Regulation of The European Parliament and of the Council on machinery products. COM(2021) 202 final. 2021/0105 (COD). Brussels, 21.4.2021.

[67] Inception impact assessment on Revision of the eIDAS Regulation – European Digital Identity (EUid)

identification schemes. In April 2021, the European Commission published a proposal for the revision of the Machinery Directive, aiming to update the health and safety requirements for machinery falling under the scope of the Directive. In this regard, the European Economic and Social Committee[68] (EESC) recommended that that cybersecurity concerns over machineries should be dealt with in a separate horizontal legislation as cybersecurity does not only depend on machine manufacturers. To this extent, the proposal listed under Annex III – Risk profiles tables the conformity essential health and safety requirements that have to be fulfilled by a machinery in order to receive a statement of conformity. Lastly, the revision of the GPSD will address product safety challenges linked to new technologies[69]. In fact, the concept of 'safety' currently spelled out in the Directive appears to be not detailed enough to protect consumers from the security gaps of connected products.

These upcoming interventions and the revision of current legislation listed in Table 11 could help to set a broad-based legislative framework aimed at covering lacunae of sector-specific initiatives and complementing the provisions of existing or forthcoming legislation. However, they will have to make use of clear cybersecurity requirements to protect citizens and organisations from the security breaches which come along with connected devices [70]. Additionally, any new EU interventions need to stay coherent with the existing legislation touching upon ICT products (e.g. **GPSD**[71], **Product Liability Directive**[72]). Ultimately, the EU should continue acting 'in a coordinated manner with a view to a horizontal and forward-looking consistent digital policy' and 'bear in mind the need to strengthen digital trust and security, which includes both ICT products and services, and to minimise fragmentation of the Single Market, aiming at an efficient, transparent and coherent European framework', as stressed by the **Council Conclusions on the Future of a highly digitised Europe beyond 2020**[73]. Table 11 below presents a list of EU legislation currently under discussion at different steps of the legislative procedure.

[68] CCMI/172 Revision of the Machinery Directive, information report Consultative Commission on Industrial Change (CCMI) on the Revision of the Machinery Directive, CCMI/172-EESC-2020

[69] Inception impact assessment on Revision of the General Product Safety Directive.

[70] COM(2018) 246 final, Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), 7 May 2020, Brussels.

[71] Directive (EC) 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety, 15 January 2002, Brussels.

[72] Directive (EEC) 85/374 of the Council of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, 25 July 1985, Brussels.

[73] Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion", 7 June 2019, Brussels.

Table 11 Upcoming EU initiatives (list not exhaustive)

ID	Legislation	Category	Sector	OLP[74] step
34	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market	Horizontal	All	Revision
35	Proposal for a Regulation on Privacy and Electronic communications, COM(2017) 10 final	Horizontal	All	First reading
36	Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety	Horizontal	All	Revision
37	Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC	Sectoral	Machinery	Revision

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

Overall, it appears that the existing EU regulatory framework may not be able to tackle specifically the problem related to the rising cybersecurity risk in ICT products. The review of horizontal and sectoral legislation as well as the new proposed legislation may change the legislative framework related to ICT products cybersecurity. However, to increase the safety for ICT products and services, cybersecurity must be thought all along the lifecycle of the connected objects, from the design, manufacturing, distribution, to the usage phase including resale and until the end of life or even the recycling of ICT products. Every risk emerging at each of these phases must be anticipated and treated with technological specificities and constraints of the whole ICT Products value chain in mind. In conclusion, the ICT industry is a primary driving force behind the development and use of technologies designed to increase internet security, therefore, EU policies and legislation should foster its growth promoting cooperation between Member States and especially guaranteeing its security through the identification of a common approach to tackle cross-border ICT threats [75].

2.1.4 National legislation

National legislation and national initiatives may also be considered relevant in relation to cybersecurity for ICT products.

For instance, in Germany, on 23 April 2021, the German Bundestag adopted the **IT Security Act 2.0 or IT-Sicherheitsgesetz 2.0**. This legislation aims to strengthen the national IT security standards by amending existing laws. While assigning to the German Federal Office for Information Security new consumer protection responsibilities such as the establishment of mandatory minimum standards for IT security, the Act also introduces a voluntary IT security label aimed to provide consumers with more transparency about security-relevant IT product characteristics[76]. The Act imposes new reporting obligations on manufacturers of IT products, mandating them to report malfunctions as soon as they identify security gaps even before the customer is aware of them. Additionally,

[74] The acronym OLP stands for ordinary legislative procedure.

[75] European Parliament (2012), Resolution of 12 June 2012 on critical information infrastructure protection, P7_TA(2012)0237.

[76] Hogan Lovells (2021). German Bundestag adopts IT Security Act 2.0 - update for companies. Information available at: https://www.lexology.com/library/detail.aspx?g=b7c7d967-58cb-49d6-bdca-7d4761d3f4ab

the **Cash Register Security Regulation or Kassensicherungsverordnung**[77] entered into force on 1 January 2020 with the aims to regulate the technical requirements for computerised cash register systems and protect cash transactions against tampering of companies' basic digital records.

Countries like **Italy**[78] **and France**[79] have recently published national strategies on AI with the aim to assess the AI markets, improve the AI education ecosystem and develop an ethical framework for a transparent use of AI. In some case, national legislation even fostered the development of EU initiatives, as it happened for the French **Medical devices cybersecurity guidelines**[80]. The *Agence nationale de sécurité du médicament et des produits de santé* (ANSM) released draft guidelines on cybersecurity for producers of medical devices in July 2019. This initiative served as a base to draft the guidelines of the Medical Device Regulation at the EU level[81].

However, albeit important, these national initiatives bear the risk of fragmenting the European Digital Single Market. A fragmented landscape damages the Union making it difficult for European companies to compete on the global level and reducing the choice of viable cybersecurity technologies for citizens, as explained in the **European Commission's communication**, **COM (2009) 149 final**[82]**.** Ultimately, despite the existing horizontal, sectoral and national legislation, the risks related to the fragmentation of ICT security products and services are still relevant today and, therefore, there is a strong need to improve cooperation across Member States in order to **strengthen Europe's Cyber Resilience System**[83].

Table 12 below presents a list of existing national legislation tackling cybersecurity for ICT products. The table also illustrates which of them have been drafted as the result of the transposition of EU law.

Table 12 National legislation in relation to cybersecurity for ICT products (list not exhaustive)

ID	Legislation	Member State	Transposing EU law
1	Law 112(I)/2004 on the Regulation of Electronic Communications and Postal Services	Cyprus	Yes
2	Law 89(I)/2020 on the Security of Network and Information Systems Security	Cyprus	Yes
3	Government Decree on Security Classification of Documents in Central Government (1101/2019)	Finland	No
4	Act on Information Management in Public Administration	Finland	Yes
5	Law on international information security obligations	Finland	No
6	Law on information security auditing bodies	Finland	No
7	Law on evaluation of information systems and telecommunication arrangements used by governmental authorities	Finland	No
8	Criteria to Assess the Information Security of Cloud Services (PiTuKri) *	Finland	No
9	KATAKRI 2015 - Information security audit tool for authorities *	Finland	No

[77] Information available at : https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Verordnungen/2017-10-06-KassenSichV.html

[78] Information available at : https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf

[79] Information available at : https://www.aiforhumanity.fr/en/

[80] Information available at : https://ansm.sante.fr/var/ansm_site/storage/original/application/d774458aa87b52d2a32d736bdc9ab526.pdf

[81] Information available at : https://ec.europa.eu/docsroom/documents/41863

[82] COM (EU) (2009) 149 final, Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Brussels, 30.3.2009.

[83] COM (EU) (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, Brussels, 29.1.2020.

ID	Legislation	Member State	Transposing EU law
10	Finnish Cybersecurity label for Consumer IoT products	Finland	No
11	Laki terveydenhuollon laitteista ja tarvikkeista (629/2010)	Finland	Yes
12	Cybersecurity of medical devices integrating software during their life cycle*	France	No
13	Volume V of the Social Insurance Code	Germany	No
14	Medical Devices Act	Germany	Yes
15	Energy industry Act	Germany	Yes
16	Federal Law on Metering Point Operation	Germany	No
17	Act on making products available on the market (Product Safety Act)	Germany	Yes
18	Telecommunications Act	Germany	Yes
19	The Fiscal Code of Germany	Germany	No
20	Kassensicherungsverordnung – regulation on security of cash registers	Germany	No
21	Road Traffic Act	Germany	No
22	Act on the Federal Office for Information Security	Germany	No
23	Federal Data Protection Act	Germany	No
24	Cybersecurity requirements and certifications on gambling machines	Germany	No
25	Cabinet of Ministers Regulation No. 442 “Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements” (adopted on July 28, 2015)	Latvia	Yes
26	Law on Electronic Identification of Natural Persons	Latvia	Yes
27	Cabinet of Ministers Regulation No. 560 “Regulations Regarding the Technical and Organisational Requirements for the Qualified and Qualified Increased Security Electronic Identification Service Provider and the Service Provided Thereby” (adopted on September 19, 2017)	Latvia	Yes
28	Cabinet of Ministers Regulation Nr. 689 “Procedures for Registration, Conformity Assessment, Distribution, Operation and Technical Supervision of Medical Devices” (adopted on November 28, 2017)	Latvia	Yes
29	Cabinet of Ministers Regulation No. 317 “Procedure for Establishment, Supplementation and Maintenance of the Register of Medical Practitioners and Medical Support Persons” (adopted on May 24, 2016).	Latvia	No
30	Cabinet Regulation No. 170 “Regulations on the Register of Medical Institutions” (adopted on March 8, 2005).	Latvia	No
31	Cabinet of Ministers Regulation No. 60 “Regulation Regarding Mandatory Requirements for Medical Treatment Institutions and Their Structural Units” (adopted on January 20, 2009)	Latvia	No
32	Cabinet of Ministers Regulation Nr. 134 “Regulation Regarding the Unified Electronic Information System of the Health Sector” (adopted on March 11, 2014)	Latvia	No
33	Unified Surveillance Information System	Latvia	No
34	Telecommunications Law	Poland	Yes
35	Regulation of the Minister of Digital Affairs of 4 December 2019 on organisational and technical conditions for entities providing cybersecurity services and internal organisational structures of operators of essential services responsible for cybersecurity	Poland	Yes
36	Law 46/2018, of August 13 2020	Portugal	Yes
37	Administrative order 8877/2017, of October 9, 2017, establishes the governance model on the implementation of a cybersecurity policy in the Health sector	Portugal	No
38	Regulation 303/2019, of April 1, 2019, on the security and integrity of the networks and electronic communications services	Portugal	Yes
39	Decree Law 52/2020, of August 11, 2020, establishes the data controller and regulates the intervention of the MD in the stayaway COVID system	Portugal	No
40	Decree Law 91/2018, of November 12, 2018, approves the new legal regime for payment services and electronic currency	Portugal	Yes

ID	Legislation	Member State	Transposing EU law
41	Decree Law 142/2019, of September 19, 2019, approves the national program of civil aviation security	Portugal	Yes
42	General Law of Telecommunications (2014). At now it is in public approbation the new law that transposes the new European telecommunications directive.	Spain	Yes
43	Electronic Signature Law (2003)	Spain	Yes
44	Law of Use of ICT products in Justice Administration (2011)	Spain	Yes
45	Law of Network Information Security (2018) that transposes the NIS Directive	Spain	Yes
46	EU regulation 2019/881, relative to ENISA and the certification of cybersecurity of information and communication technologies (attached to this email), and there are several articles that refer to the certification of ICT products (Arts. 51, 52 , 53, 54 and 55).	Spain	Yes

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

* Not a legislative act but document published by a national authority aimed to increase the level of cybersecurity of ICT products.

Furthermore, according to a short survey conducted by the Project Team in November 2020, several Member States (e.g. Cyprus, Czech Republic, Netherlands) trust that a new EU certification scheme, in line with the provisions of the Cybersecurity Act, will strengthen ICT product cybersecurity within their national borders. On the other hand, other Member States (e.g. Estonia, Germany) are taking a proactive approach towards ICT product cybersecurity in some sectors (e.g. energy, automotive). For instance, in **Germany**, the **draft regulation on autonomous driving** will request to car manufacturers to clearly define spatial and technical conditions that allow their vehicles to drive autonomously. Once these conditions are approved by the designated supervisory authority, the manufacturers shall prove that these requirements are met in a certain area before placing the vehicles into circulation. In more general terms, the regulation will include the functionality, testing procedures and approval of autonomous driving functions, while considering important cybersecurity aspects.

Finally, when looking outside the European Union, two new United Nations **Regulations on Cybersecurity and Software Updates**[84] have been issued. These will be used as guidelines for addressing cybersecurity concerns, as presented in Box2 below.

[84] Information available at : https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html

Box 2 United Nations Regulations on Cybersecurity and Software Updates

In June 2020, the United Nations Economic Commission for Europe (UNECE) adopted two new UN Regulations on Cybersecurity[85] and Software Updates[86] that will help the world to address cyber risks (e.g. hackers accessing electronic systems of a vehicle) by setting performance and audit requirements for car manufacturers. These regulations represent the first ever internationally harmonised and binding norms in the sector of automated vehicles.

The main areas of interventions of the new regulations are:

Management of vehicle cyber risks;

- Definition of a security by design approach to vehicles;
- Detection of and response to cybersecurity incidents across vehicle fleet; and
- Provision of safe and secure software updates.

Within the EU, while the new regulation on cybersecurity will be mandatory for all the new types of vehicles starting from July 2022, the entry into force for all new vehicles produced is July 2024.

2.2 Legislative gap analysis

As mentioned in the previous sections, there are numerous EU and National legislation that address issues related to the cybersecurity of ICT products. However, the current EU legislative framework was not initially designed to address those topics. The analysis shows that the scope is too narrow and cannot fully guarantee the liability, cybersecurity and safety of ICT products available in the Single Market. For instance, gaps have been identified in relation to the requirements for manufacturers of ICT products or the operators and processors of these products. Therefore, the Project Team conducted a gap analysis to better identify such gaps.

A gap analysis is a management tool that compares actual performance against desired performance and thereby identifies any gap between the two. The second aspect of a gap analysis is the identification of the potential options for closing the identified gap and ultimately the agreement of preferred solutions. This second aspect is tackled through Task 4, which identifies the policy options available to close the identified gaps between the expected level of cybersecurity for ICT products as identified in Task 3, and the current EU legislative framework.

The gap analysis performed by the Project Team follows several research questions:

- What are the products in scope of the selected list of EU legislation?
- What is the level of granularity in the definition of the products in scope?
- What are the requirements/provisions addressed in relation to cybersecurity for ICT products?
- What is the level of granularity of the requirements/provisions?
- What are the implementation measures of the requirements – mandatory or voluntary?
- What is the geographical scope of the legislation? and;

[85] Information available at : http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[86] Information available at : https://undocs.org/ECE/TRANS/WP.29/2020/80

- What are the gaps in relation to the cybersecurity objectives set in the Cybersecurity Act Article 51?

The scope of the gap analysis consists of 37 pieces of EU legislation concerning ICT products as presented in Table 10 and Table 11 in the previous section. This set of legislation includes all legislation related to the NLF, as well as legislation with a strong link with cybersecurity and data protection, which can affect very indirectly manufacturers (e.g. eIDAS Regulation, GDPR, Directive on Security of Network and Information Systems, RED, GPSD).

The main purpose of the gap analysis is to support the identification of the key problems currently faced in relation to the cybersecurity for ICT products available across the EU. The complete gap analysis is structured in the form of an Excel database that provides information on the products in scope, by identifying the relevant articles, the articles addressing cybersecurity for manufacturers or service providers, the mandatory/voluntary aspect of the requirements, and other aspects that contribute to the study.

Finally, the Project Team compared the cybersecurity objectives set in the Cybersecurity Act Article 51, against the identified requirements of the EU legislation in scope. This analysis used as a basis the Cybersecurity Act as this is one of the most recent, up-to-date, and relevant EU legislation that covers cybersecurity for ICT products at broad spectrum. The cybersecurity objectives of Article 51 also provide a comprehensive list of high-level cybersecurity requirements for ICT products, such as protection against unauthorised access or disclosure of information, or verification, or to follow the security by default principle. In the rest of the study, the completeness of the security objectives for ICT Products of the Cybersecurity Act will be challenged in Task 3; it is used here as a preliminary point of reference for the legislative gap analysis. Furthermore, taking the Cybersecurity Act as a point of reference does not imply any set orientations on the policy options that will be detailed in Task 4, nor on the need of certification for ICT products at that stage. Table 13 below presents the full list of cybersecurity objectives set in Article 51. Additionally, the gap analysis identified articles from the selected list of EU legislation, that could be linked to "market surveillance", as this aspect in relation to ICT products, could indirectly cover cybersecurity and risk management for ICT products.

Table 13 Article 51 Security objectives of European cybersecurity certification schemes

Reference	Comprehensive objective	Objective as stated in the Cybersecurity Act
a)	Protection against accidental or unauthorised storage, processing, access and disclosure	to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;
b)	Protection against accidental or unauthorised destruction, loss or alteration or lack of availability	to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
c)	Authorisation to access data and services	that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
d)	Identification of dependencies and vulnerabilities	to identify and document known dependencies and vulnerabilities;
e)	Record of access	to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
f)	Verification of access	to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
g)	Verification of the absence of vulnerabilities	to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
h)	Restauration of availability	to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
i)	Security by default and design	that ICT products, ICT services and ICT processes are secure by default and by design;
j)	Secure update of software and hardware	that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

An additional focus is put on understanding whether the EU legislation in scope are tackling equally security and safety for the products or services identified in their scope.

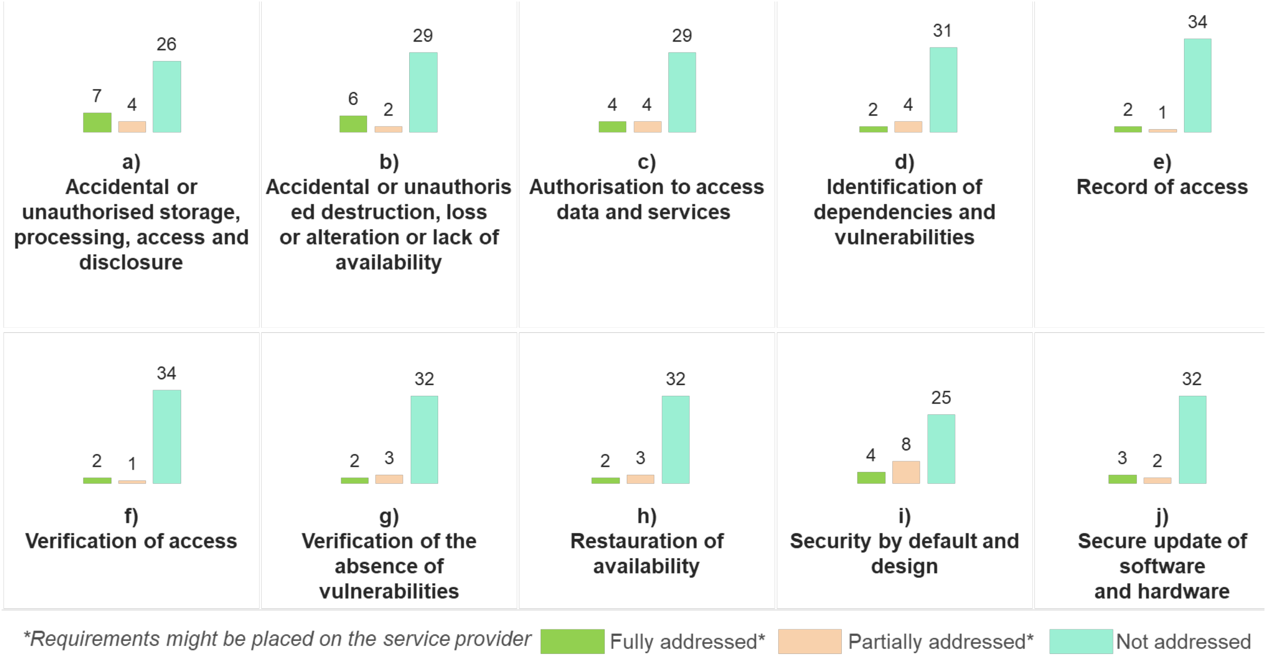
Based on the conduced gap analysis on the 37 EU legislation in scope, the following sections present the identified seven key findings that help us to better scope the key problems, key drivers, and main consequences:

- **Key Finding 1:** The current EU legislative framework does not cover all security objectives of the Cybersecurity Act, described in Table 13, with fragmentation and gaps related to cybersecurity requirements for ICT products;
- **Key Finding 2**: The legislation related to the NLF do not address fully the cybersecurity requirements for ICT products set in Article 51;
- **Key Finding 3**: Some cybersecurity requirements addressed to service operators can affect indirectly the cybersecurity level of ICT products used to operate the service, without setting obligations on the manufacturers;
- **Key Finding 4**: There are different levels of granularity in the definition of the scope of products covered by the EU legislative framework;
- **Key Finding 5**: There are different levels of granularity of cybersecurity requirements in the legislation in scope;
- **Key Finding 6:** Several pieces of legislation require the manufacturer or service provider to issue “notifications” in case of a cybersecurity breach or risk, which is an objective that is not present in the Cybersecurity Act; and
- **Key Finding 7:** The safety aspects of products in scope are overall more addressed than the security aspects.

Key Finding 1 – The current EU legislative framework does not cover all security objectives, with fragmentation and gaps related to cybersecurity requirements for ICT products

Overall, only a limited set of EU legislation addresses explicit cybersecurity requirements for ICT products. **On average, a legislation addresses approximately two of the 10 cybersecurity objectives** set in Article 51. Furthermore, in less than 30% of the studied legislation, the cybersecurity objectives are partially or completely addressed. Figure 3 below presents an overview of the 37 studied EU legislation and the level of coverage (i.e. full, partial, not addressed) with regard to the cybersecurity objectives set in Article 51. The gap analysis overview maps requirements set in the different EU legislation that are addressed to both manufacturers and services providers.

Figure 3 Gap analysis overview



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), GAP ANALYSIS BASED ON LITERATURE REVIEW.

Furthermore, the analysis shows that neither any of the horizontal legislation in scope, nor a combination of horizontal and specific legislation can cover the full spectrum of cybersecurity objectives from Article 51 in relation to all types of products. For example, consumer goods not processing personal data (e.g. IoT devices) are not covered by GDPR nor by the NIS Directive and would have to answer to the Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, mandating the need to provide security updates. Another example is when ICT products handle non-personal data (e.g. financial data, critical-infrastructure related data), they do not fall under the GDPR as the legislation does not cover the products in scope. The Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods, is the only one horizontal legislation that addresses fully one of the 10 security objectives of Article 51 – objective j) Secure update of software.

Out of the total 37 pieces of EU legislation in scope, apart from the Cybersecurity Act, there are only five with partial or complete coverage of five or more of the cybersecurity objectives, which are presented below:

- General Data Protection Regulation[87];
- Regulation (EU) 2017/745 on medical devices[88];
- Regulation (EU) 2017/746 on in vitro diagnostic medical devices[89];

[87] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[88] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices

[89] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices

- RED[90]; and
- Measuring Instruments Directive[91].

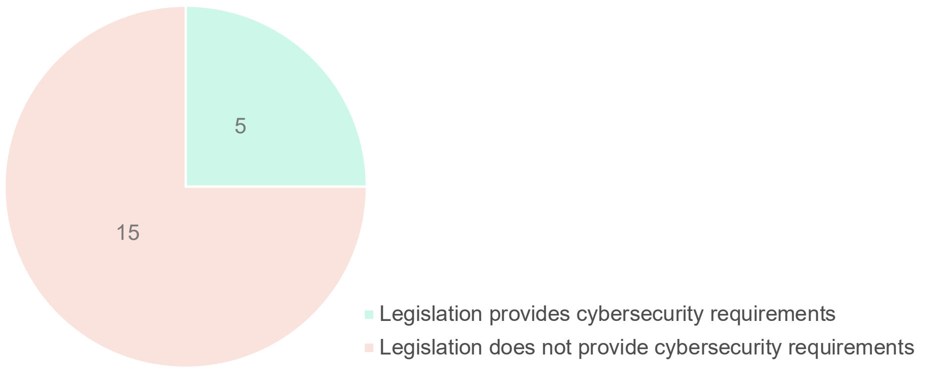
The requirements set throughout national legislation mandated by European Union legislation are not in the scope of this study. For example, the Directive 2016/1148/EU on security of network and information systems (NIS Directive) do not address any of the security objectives set in Article 51, while national legislation mandated by the NIS Directive might address partially or completely some of the objectives.

Key Finding 2 – Legislation related to the NLF does not address fully the cybersecurity requirements for ICT products set in Article 51

The NLF is a legislation package adopted in 2008 to improve the functioning of the internal market and strengthen the conditions for placing products on the European market. It addresses notably certain requirements for products in scope, obligations on economic operators, conformity assessments for products placed on the market, accreditation and market surveillance mechanisms.

Our analysis on the gaps against the cybersecurity objectives set in Article 51, shows that **15, out of 20 NLF pieces of legislation, do not address cybersecurity and are not covering any of the cybersecurity objectives. Instead, these address risk as a global and generic term through market surveillance** (e.g. need to notify authorities in case of risks, remove the product from the market in case of product failure). It could be argued that the lack of information about the security of product might represent a health or safety risk for a person or the society at large. However, this is not explicitly mentioned within the legislative text. Figure 4 presents the distribution of NLF legislation in terms of products' security requirements.

Figure 4 NLF legislation addressing Article 51 Cybersecurity objectives



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), GAP ANALYSIS BASED ON LITERATURE REVIEW.

[90] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment

[91] Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments

The following five pieces of NLF legislation provide some cybersecurity requirements for ICT products, although none of them address all security objectives:

- Regulation (EU) 2017/745 on medical devices[92];
- Regulation (EU) 2017/746 on in vitro diagnostic medical devices[93];
- RED[94];
- Non-automatic weighing instruments Directive[95]; and
- Measuring instruments Directive[96].

Finally, some of the products regulated by NLF-related legislation are unlikely to fit the definition of an ICT product in their current form (e.g. personal protective equipment, transportable pressure equipment, appliances burning gaseous fuels). This kind of products could be exposed in the future to cybersecurity risks due to the continuous digitalisation and connectivity of products. Therefore, the Project Team has not considered this product to be out of scope for the study.

Key Finding 3 – Some cybersecurity requirements addressed to service operators can affect indirectly the cybersecurity level of ICT products used to operate the service, without setting obligations on the manufacturers

On the one hand, in 23, out of 37 pieces of legislation in the scope of this study, requirements are addressed directly to ICT products covered by the legislation. On the other hand, seven pieces of legislation cover services rather than products. In those cases, one could argue that the requirement indirectly applies to products too. Indeed, the service provider is entitled to decide on the type of safeguards to be put in place on the product that is used to deliver the service. Figure 5 below presents the distribution of legislation on this matter.

[92] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)

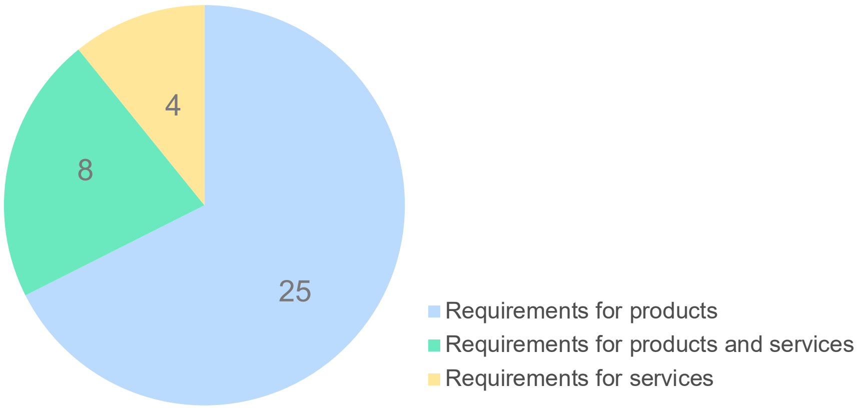
[93] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.)

[94] irectiv e 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making av ailable on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance

[95] Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments

[96] Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast) Text with EEA relevance

Figure 5 Distribution of legislation based on their cybersecurity requirements' scope



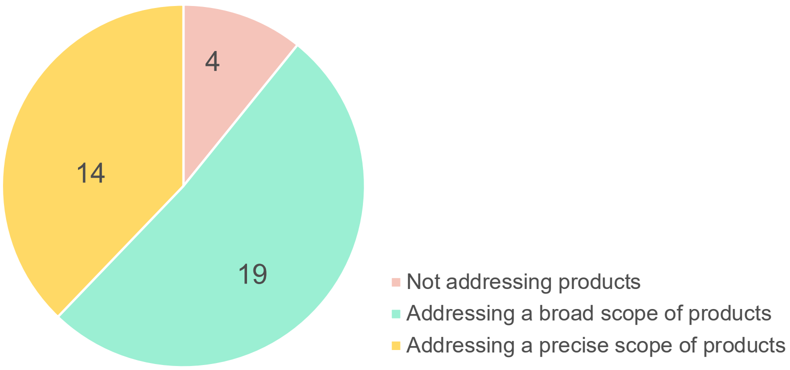
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), GAP ANALYSIS BASED ON LITERATURE REVIEW.

A good example of indirect requirements towards the product is the GDPR. The GDPR only addresses Data Controllers and Data Processors, and does not address the product manufacturers, even if their products store, transmit or process personal data. It is up to the Data Controllers and Data Processors to cover such security obligation both in the procurement and operation processes (e.g. delivering the services). However, GDPR does not set requirements directly on ICT products. Instead, the requirements are set by Data Controllers subject to the legislation. As a consequence, Data Controllers may impose very different requirements depending on the ICT product concerned, leading to misalignments ICT product cybersecurity and additional complexity for the manufacturers. Another example that could be mentioned is the NIS Directive, which sets requirements at national level that address essential services only. Similarly, it is up to the Operators of Essential Services to identify and configure the underlying ICT products which allow compliance with the Directive and the transposed legislation. Additionally, National Competent Authorities might also be involved in the implementation of such national legislation and could provide guidance in the selection of products used by Operators of Essential Services, such as through certification. This issue can be correlated with Problem 2, the **insufficient understanding among users (e.g. citizens and companies) concerning the level of cybersecurity for ICT products,** as defined in Section 2.3. In fact, while the service operators need to ensure the security of the products they use, it remains difficult for them to adequately assess the level of security of such products.

Key finding 4 – There are different levels of granularity in the definition of the scope of products covered by the EU legislative framework

There are different approaches in the way the scope of products is addressed in the different legislation. As presented in Figure 6 below, out of 37 pieces of legislation, 14 have a precise set of products in scope, while 19 of them address a broad set of products in the Common Market.

Figure 6 Distribution of legislation based on their products' scope definition



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), GAP ANALYSIS BASED ON LITERATURE REVIEW.

For example, legislation with a specific scope of products is often present in the NLF, where criteria for applicability of the legislation have been set very precisely. This is the case of the products regulated in the Recreational craft and personal watercraft Directive[97], providing both a precise scope on what kind of watercraft would fall under the directive and a comprehensive list of exceptions.

On the other hand, other legislation is not as precise and addresses a larger scope of ICT products. Examples can be seen in the GPSD[98], which address all consumer products placed on the market, or in the Unfair Commercial Practices Directive[99]. Other legislation with a broad scope is the type of legislation addressing specific sectors, such as the Civil Aviation Regulation[100].

It has to be noted that the definition of a broader scope for products can be explained as such directives were initially developed to address services (see Key Finding 3) or products in general, and not specifically ICT products.

Key finding 5 – There are different levels of granularity of cybersecurity requirements in the legislation in scope

In cases of legislation addressing security requirements for products, the analysis shows that these requirements are less precise and less descriptive compared to the security objectives of Article 51.

An example of a legislation where there is a generic and less precise requirement for a product is the Civil Aviation Regulation100, where the only requirement presented regards the design of the aircraft and its underlying components refers to minimising hazards due to information security threats:

[97] Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft

[98] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

[99] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council

[100] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency

"Appendix II

1.3.1. The aircraft must not have design features or details that experience has shown to be hazardous.

1.3.5. Design precautions must be taken to minimise the hazards to the aircraft and occupants from reasonably probable threats, including information security threats, both inside and external to the aircraft, including protecting against the possibility of a significant failure in, or disruption of, any non-installed equipment."

On the other hand, other legislation provides more details and guidance on the requirements for the products in scope. An example for such legislation is the eIDAS Regulation[101], which provides specific requirements for electronic signature creation devices.

"Annex II

Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

(b) the electronic signature creation data used for electronic signature creation can practically occur only once;

(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

(a) the security of the duplicated datasets must be at the same level as for the original datasets;

(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service."

[101] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

Key finding 6 – Several pieces of legislation require the manufacturer or service provider to issue "notifications" in case of a cybersecurity breach or risk, which is an objective that is not present in the Cybersecurity Act

Several pieces of legislation require the manufacturer or service provider to issue "notifications" to customers or national authorities when a cybersecurity breach occurs. However, this requirement is not part of the Article 51. An example of such regulation is the Directive on privacy in the electronic communications[102], in which Article 34 requests 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.".*

Other legislation may require the manufacturer to contact the relevant national authority, such as the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, in which Article 40 requires that:

> *"Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.".*

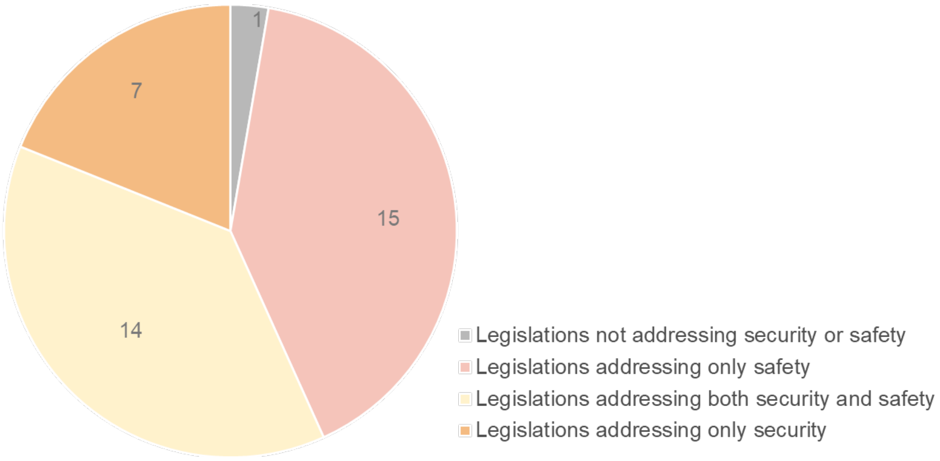
Additionally, legislation connected to the NLF mandates the need to contact authorities in case a risk is identified on a product. However, cybersecurity risks are not explicitly mentioned in the legislation as mentioned in Key Finding 2.

Key finding 7 – The safety aspects of products in scope are overall more addressed than the security aspects

The gap analysis points out that 15 out of the 37 pieces of legislation address only safety through their provisions, while 14 pieces of legislation address both security and safety, and seven address only security and do not mention safety. The predominance of safety is especially true for the NLF, were 12 out of 20 pieces of legislation connected to the NLF address only safety, and eight address both safety and security. Figure 7 below presents this distribution.

[102] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Figure 7 Distribution of legislation based on their safety or security aspects



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), GAP ANALYSIS BASED ON LITERATURE REVIEW.

2.3 Conceptualisation of the problem tree

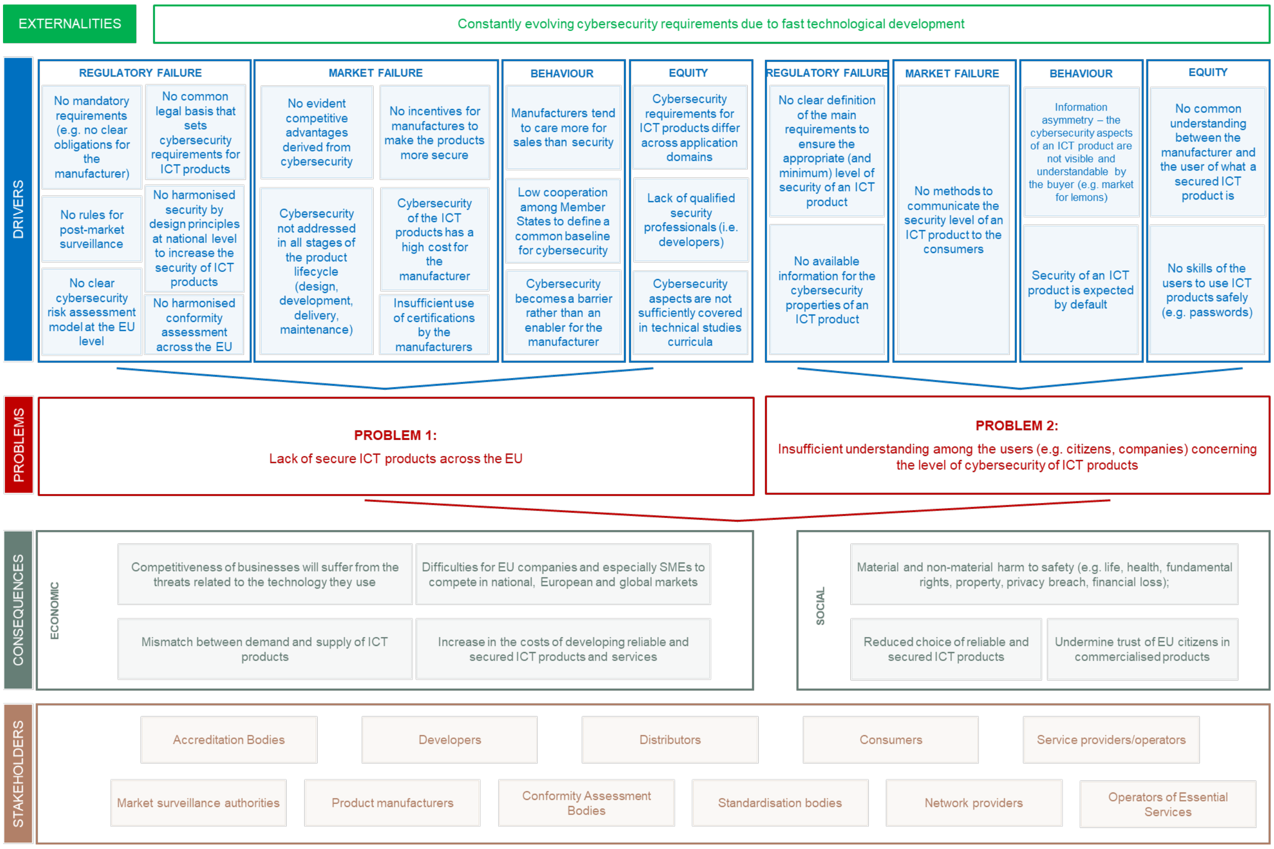
This section delves into the preliminary outline of the problem definition. For a visual description of the preliminary problem tree see Figure 8 below.

The problem tree within an impact assessment consists in reflecting on the prevalence of the problems identified in the original intervention, which are set out in the respective intervention logic, and take stock of new problems arising from new needs or changes in the policy landscape related to the cybersecurity requirements for ICT products. Desk research and evidence from conducted surveys and focus groups and, in particular, the questions on the relevance contribute to this section. The development of the problem tree follows the steps indicated in the Better Regulation Guidelines of the European Commission.

The following research questions guide this exercise:

- What are the problems?
- What is the scale of the problems?
- What are the drivers of the problems?
- Who are the relevant stakeholders?
- What are the main consequences?

Figure 8 Preliminary problem tree


EXTERNALITIES
Constantly evolving cybersecurity requirements due to fast technological development
DRIVERS
REGULATORY FAILURE
No mandatory requirements (e.g. no clear obligations for the manufacturer)
No common legal basis that sets cybersecurity requirements for ICT products
No rules for post-market surveillance
No harmonised security by design principles at national level to increase the security of ICT products
No clear cybersecurity risk assessment model at the EU level
No harmonised conformity assessment across the EU
MARKET FAILURE
No evident competitive advantages derived from cybersecurity
No incentives for manufactures to make the products more secure
Cybersecurity not addressed in all stages of the product lifecycle (design, development, delivery, maintenance)
Cybersecurity of the ICT products has a high cost for the manufacturer
Insufficient use of certifications by the manufacturers
BEHAVIOUR
Manufacturers tend to care more for sales than security
Low cooperation among Member States to define a common baseline for cybersecurity
Cybersecurity becomes a barrier rather than an enabler for the manufacturer
EQUITY
Cybersecurity requirements for ICT products differ across application domains
Lack of qualified security professionals (i.e. developers)
Cybersecurity aspects are not sufficiently covered in technical studies curricula
REGULATORY FAILURE
No clear definition of the main requirements to ensure the appropriate (and minimum) level of security of an ICT product
No available information for the cybersecurity properties of an ICT product
MARKET FAILURE
No methods to communicate the security level of an ICT product to the consumers
BEHAVIOUR
Information asymmetry – the cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons)
Security of an ICT product is expected by default
EQUITY
No common understanding between the manufacturer and the user of what a secured ICT product is
No skills of the users to use ICT products safely (e.g. passwords)
PROBLEMS
PROBLEM 1:
Lack of secure ICT products across the EU
PROBLEM 2:
Insufficient understanding among the users (e.g. citizens, companies) concerning the level of cybersecurity of ICT products
CONSEQUENCES
ECONOMIC
Competitiveness of businesses will suffer from the threats related to the technology they use
Difficulties for EU companies and especially SMEs to compete in national, European and global markets
Mismatch between demand and supply of ICT products
Increase in the costs of developing reliable and secured ICT products and services
SOCIAL
Material and non-material harm to safety (e.g. life, health, fundamental rights, property, privacy breach, financial loss);
Reduced choice of reliable and secured ICT products
Undermine trust of EU citizens in commercialised products
STAKEHOLDERS
Accreditation Bodies
Developers
Distributors
Consumers
Service providers/operators
Market surveillance authorities
Product manufacturers
Conformity Assessment Bodies
Standardisation bodies
Network providers
Operators of Essential Services

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

2.3.1 What are the problems?

Following the data collection activities performed between 9 October 2020 and 30 November 2020, namely in-depth literature review, online questionnaires to National Competent Authorities, face-to-face interviews with European Commission officials, two focus groups, one virtual workshop, and the conducted gap analysis, the Project Team has identified two main problems in relation to the need of cybersecurity requirements for ICT products:

- **Problem 1 –** Lack of secure ICT products across the EU; and
- **Problem 2 –** Insufficient understanding among users (e.g. citizens and companies) concerning the level of cybersecurity for ICT products.

Lack of secure ICT products across the EU

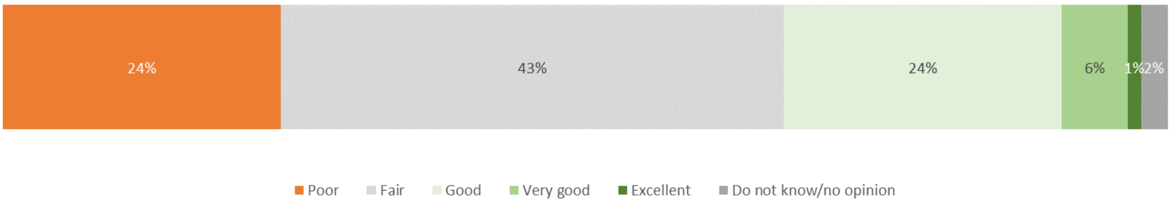
Problem 1, the lack of secure ICT products across the EU is not a recent problem. From smartphone to medical devices and gambling machines, ICT products are inherently vulnerable. These connected devices are not always protected as they can be connected to networks without anyone being aware of it[103]. In October 2016, a cyber-attack

[103] 2020 Cybersecurity Report, Check Point, 22 January 2020.

based on a malware called Mirai targeted hundreds of thousands of insecure IoT devices, bringing down websites such as Twitter, Amazon, Spotify and Netflix[104]. The next month, a variant of the Mirai malware targeted customers' home routers of Germany's telecommunication company Deutsche Telekom, resulting in a large number of home routers being hit by an outage[105]. On May 2017, several companies and organisations around the world experienced a cyber-attack by a crypto-ransomware called WannaCry. Due to its worm-spreading functionality, the ransomware needed only to have access to a system to be able to self-propagates throughout the rest of the network[106]. The same year, the malware NotPetya caused more than USD one billion worldwide. More recently, a UK consumer group organisation, which, reported several security flaws in widely-marketed smart doorbells[107]. These flaws are currently putting consumers at risk of being the target of cyber-attacks inside their homes. These are only some examples that demonstrate how the presence of insecure ICT products within the EU represents a threat to consumers as well as public organisations and private companies. Following the feedback provided by consumers associations, such as BEUC and ANEC, the issue appears to be even more paramount as the number of connected devices available within the Digital Single Market has been increasing over time[108] and the financial impact of cyber-attacks continues to grow[109].

The results of the targeted consultation partially support a general perception among stakeholders about the lack of secure ICT products across the EU (see Figure 9). Particularly, while only 31% of the respondents to the survey claims that the level of cybersecurity of ICT products is at least good (three out of five or more on the Likert scale), one quarter considers it to be poor and more than 40% assesses it as merely "fair".

Figure 9 Opinion of stakeholders on the level of security of ICT products available



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

During the data collection activities performed by the Project Team (e.g. Workshop 1 – Problem definition), some stakeholders have highlighted that certain sectors (e.g. energy) are more protected against cyber-attacks due to a more comprehensive sectoral regulation setting cybersecurity requirements and the higher attention and awareness that market operators have towards cybersecurity aspects for ICT products connected to the network. Nevertheless, while no sector appears to be risk free, consumers associations have supported the opinion that several other sectors appear to be at a higher risk of compromise due to the presence of cheaply produced ICT products[110] (i.e. 'fire and forget' approach), not designed in a secure way. For example, an

[104] ANEC, BEUC (2018); Cybersecurity for Connected Products – Position Papers, ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018

[105] Information available at : https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

[106] Information available at : https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

[107] Information available at : https://www.which.co.uk/news/2020/11/the-smart-video-doorbells-letting-hackers-into-your-home/

[108] ANEC, BEUC (2018); Cybersecurity for Connected Products – Position Papers, ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018

[109] European Court of Auditors (2019), Challenges to effective EU cybersecurity policy – Briefing Paper

[110] ANEC, BEUC (2018); Cybersecurity for Connected Products – Position Papers, ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018

electronic light bulb can be connected to a network without having procedure in place to update it with security patches.

The differences in the level of ICT product cybersecurity have also been pointed out by the results of the targeted consultation. In fact, more than one respondent out of five (26% of the total responses) argued that it is difficult to assess a generic level of cybersecurity for all ICT products marketed across the EU as a great variance persists across sectors and field of application. Particularly, while the financial sector has been indicated as a secure one, stakeholders consider IoT to be the ICT product category with lower cybersecurity level. In other words, it can be argued that the cybersecurity levels of different ICT products vary greatly depending on the variables (e.g. sector, product category) taken into consideration. The great variance of ICT product cybersecurity across sectors could explain why more than four respondents to the targeted consultation out of ten described the overall level of security of ICT products across the EU as "fair". In fact, 33% of the "fair" responses claimed that it was difficult or impossible to assess the general level of ICT products' cybersecurity due to marked differences at industry level.

Insufficient understanding among users (e.g. citizens and companies) concerning the level of cybersecurity for ICT products

Despite the huge steps undertaken in the last decade, Problem 2, insufficient understanding among users (e.g. citizens and companies) concerning the level of cybersecurity for ICT products represents another long-standing problem. During the data collection activities performed by the Project Team, several Member States (e.g. Croatia, Finland and Netherlands) have pointed out that there is no regular communication to the users (e.g. consumers) about the threats that new technologies might bring, as well as that cybersecurity is not well addressed at universities.

Despite 80% of EU businesses suffered of at least one cybersecurity incident in 2016, the acknowledgement of cyber-risks is still alarmingly low. For instance, almost seven companies out of 10 have none, or basic understanding of their exposure to cyber threats [111]. Moreover, while functionalities and ergonomics of an ICT product are the main drivers of consumer decisions, consumers do not have incentives to base their purchase decisions taking into account the cybersecurity aspects. For instance, according to Eurostat, more than one individual out of five has never restricted or refused access to personal data, when using or installing an app on a smartphone in 2018[112]. The problem is even more relevant as the continuous technological development disrupts the ways connected products interact with each other, making it difficult, even for informed citizens, to understand the possible cyber threats.

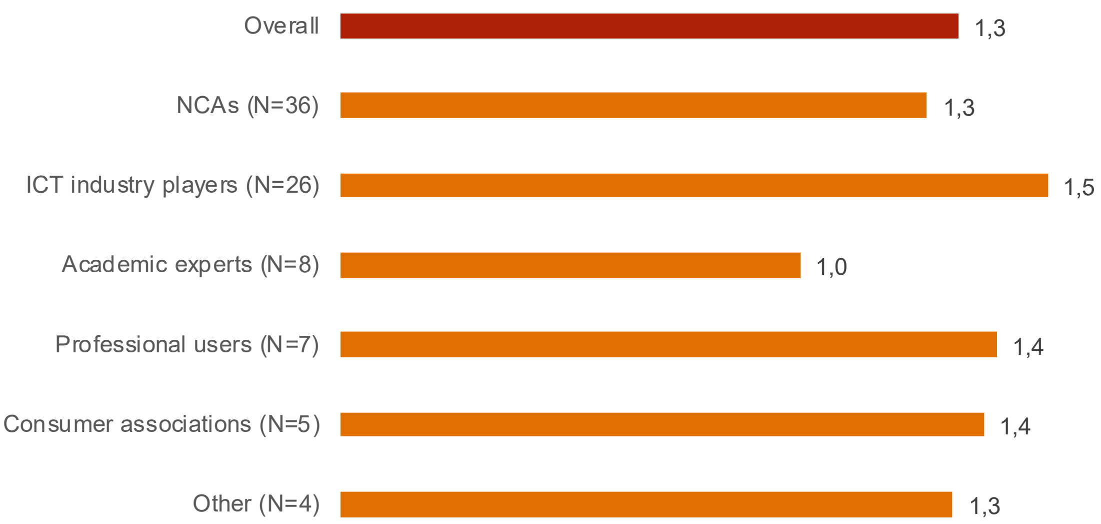
During the targeted consultation respondents were asked about their perception concerning the level of understanding of users on the cybersecurity of ICT products. Following the feedback received from stakeholders,, respondents claimed that there are major differences in the level of understanding among users. Respondents believed that the level varies greatly depending on the users under analysis. Particularly, while only 3% of the respondents defined the level of understanding of regular users (see Figure 10) as "good" or "very good", more than

[111] European Court of Auditors (2019), Challenges to effective EU cybersecurity policy – Briefing Paper

[112] Information available at : https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_sp/default/table?lang=en

half of the responses (54%) to the targeted consultation claim that professional users possess such level "good" or "very good" (see Figure 11). Furthermore, whereas only 11% of the stakeholders believe that professional users have a poor level of understanding of ICT products' cybersecurity, seven responses out of 10 indicate a poor level of understanding for regular users. Interestingly, not a single respondent considered the level of understanding being "excellent" for both types of users[113].

Figure 10 Level of understanding (awareness) among regular users[114]

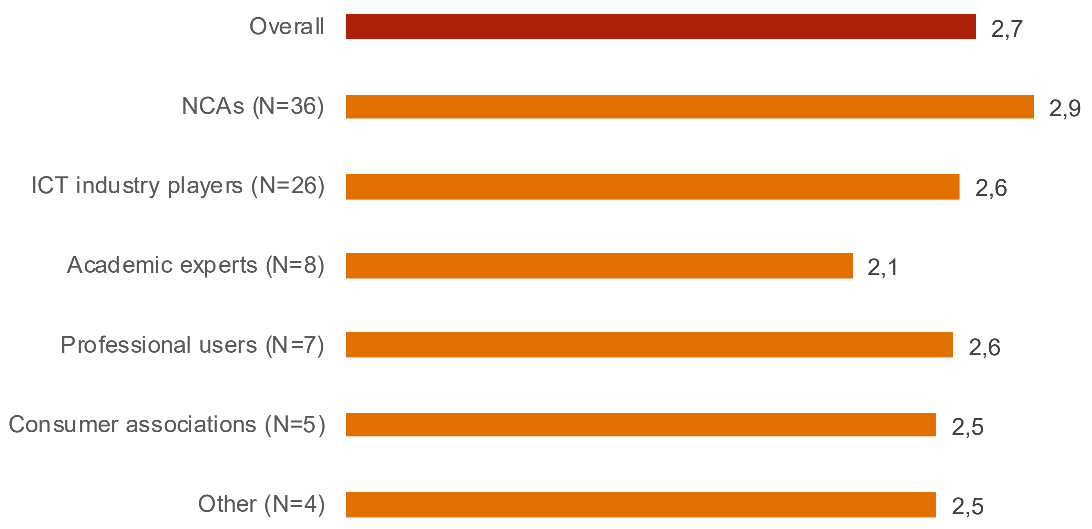


SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

[113] As highlighted by Annex V – Target Consultation Results, when assessing the level of understanding both of regular and professional users through a Likert scale (1="Poor" and 5="Excellent"), professional users get to 2,7 out of 5 while regular users score only 1,3.

[114] Other stakeholders' group lacking enough responses to be representative are present in Annex V – Target Consultation Results.

Figure 11 Level of understanding (awareness) among professional users[114]



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Moreover, in the view of the respondents to the targeted consultation, relevant differences exist among professional users depending on the sector as well as the ICT device category and the intended use of the ICT product. For instance, when asked to motivate their reply to the overall level of understanding among professional users, some respondents belonging to the national competent authorities' stakeholder group highlighted that SMEs are relatively less aware than large companies as they possess less resources to put into place comprehensive cybersecurity policies.

In addition, during the first workshop, relevant stakeholders noted that Problem 2 cannot be considered at the same level as Problem 1. They argued that some users cannot be made aware of cybersecurity concepts and thus, it is important to insist on principles such as security by design and security by default to be implemented in a mandatory way. Furthermore, it was also highlighted that Problem 1 is more important and easier to address by a regulatory intervention than Problem 2. The latter represents the fundamental economic driver for market failure of Problem 1.

Despite that, the data stemming from the desk research [115] [116] as well as the evidences collected during interviews and the focus groups suggest that not only consumers but also developers and manufacturers are not sufficiently aware of safety and cybersecurity risks posed to and by ICT products. Therefore, Problem 1 and Problem 2 should be addressed with the same level of importance by a future policy intervention.

[115] ENISA (2017). Baseline Security Recommendations for IoT. Available at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[116] ENISA (2019). Opinion Consumers and IoT security – ENISA Advisory Group. Available at: https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

2.3.2 What is the scale of the problems?

The Project Team analysed the information gathered through desk research and data collection activities in order to assess the magnitude and EU dimension of the two identified problems. The purpose of this exercise is to explore the relevance of possible cross-border effects or obstacles to the smooth functioning of the Digital Single Market.

The lack of secure ICT products across the EU (i.e. Problem 1) may have tangible cross-border impacts, representing a barrier to the smooth functioning of the Digital Single Market. Such impacts depend on the intended use of the ICT product, its context of use and the specific risks which it is subject to. For instance, while the most common negative consequences concern the lack of availability, the lack of integrity, the compromise of confidentiality, as well as physical harm (e.g. car incident) in the case of cyber-physical systems, a cyber-attack to an ICT product part of a critical system could lead to the disruption of business continuity and the block of cross-border economic and social activities.

The EU Single Market accounts for approximately 450 million consumers where many products on the EU market are subject to harmonised rules meant to protect consumers against various harms (CE marking). However, as regards cybersecurity, no similar comprehensive rules are in place and, as acknowledged by the European Court of Auditors [117], the lack of information towards the users about cybersecurity, makes it even more difficult to protect them against such risks (i.e. **Problem 2**). An illustrative example of the cross-dimensional aspects of the lack of awareness of certain products' risks and how a regulation could help to prevent such risks, is the tobacco industry. Directive 2014/40/EU on the sale of tobacco [118], introduces specific labelling rules for the manufactures aiming to raise awareness of health risks.

Following the information collected during the data collection activities, the reasons underpinning the cross-border aspects of the problems concern the very nature of ICT products, and particularly:

- **Strong interdependencies among ICT products** – The security of a connected product relies on the different security levels of each product connected to a certain system;
- **Cross-sectoral use of ICT products** – ICT products and digital components (e.g. software libraries, microprocessors) are often reused in several different products across various sectors with different risk profiles;
- **Cross-country connection** – Cybersecurity threats are nearly always cross-border. One cyber-attack on critical infrastructure in one country can affect the EU as a whole.

By digging more into the scale of the problems, it is evident from the opinion expressed by some professional associations, such as Orgalim, that while putting forward several initiatives to increase the level of ICT products cybersecurity at the national level, Member States may end up hindering or interfering with the free circulation of goods within the Single Market by mandating companies to adapt the design of their connected products [119].

[117] European Court of Auditors (2019), Challenges to effective EU cybersecurity policy – Briefing Paper

[118] Directive 2014/40/EU of The European Parliament and of The Council, of 3 April 2014, on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC.

[119] Orgalim (2019), Position Paper - Building a real European Single Market for Cybersecurity: A call for a consistent approach – guiding principles

According to a recent communication from the European Commission, seven SMEs out of 10 that tried the existing mutual recognition system for non-harmonised goods were faced with a market access denial decision[120]. The presence of public rules and requirements represents one of the main obstacles for businesses, particularly innovative SMEs[121]. Following the input from National Competent Authorities, it is possible to notice that some Member States (e.g. Czech Republic and Netherlands) currently understand and support the need for a joint action at the EU level as a mean to increase cybersecurity for connected products.

2.3.3 What are the drivers of the problems?

In order to address the problems, underlying drivers shall be identified. As a result of both, desk research and data collection activities, the Project Team identified several drivers. These problem drivers have been shortlisted and subsequently categorised under the following four sub-groups:

- **Regulatory failure**, e.g. absence of government intervention or failure of current interventions to address an issue fails to solve it or creates a new problem;
- **Market failure**, e.g. individuals or firms impose costs on others for which the market assigns no price;
- **Equity**, e.g. equity of endowments, processes and outcomes are preferred over efficient ones; and
- **Biased behaviours**, e.g. individuals and/or market operators do not base their decision on their interests.

It is worth noting that several of the problem drivers are interlinked. While highlighting all the possible connections among problem drivers has not been completely possible, the Project Team has analysed through desk research the cases where such link is more evident.

There are several drivers underpinning **the lack of secure ICT products across the EU (i.e. Problem 1).** As a result of the extensive input collected from relevant stakeholders, the Project Team has identified three main **regulatory failures** namely:

- The absence of mandatory requirements (e.g. no clear obligations for the manufacturer);
- The lack of common legal basis that sets cybersecurity requirements for ICT products;
- The absence of rules for post-market surveillance, with regards to cybersecurity.

Regarding the absence of mandatory requirements, while setting out key security objectives for ICT products that European cybersecurity certification schemes shall aim to address, the Cybersecurity Act did not bind companies with the adoption of such schemes[122]. Hence, some consumers associations, such as BEUC and ANEC, raised the concern that the voluntary nature of the cybersecurity scheme is expected to have limited reach[123] and does not

[120] European Commission (2020) Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions – Identifying and addressing barriers to the Single Market {SWD(2020) 54 final}

[121] Ibid

[122] 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 on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, 7 June 2019, Brussels.

[123] German Institute for International and Security Affairs (2019), The EU's Regulatory Approach to Cybersecurity, Research Division EU / Europe | WP NR. 02, October 2019

ensure that the cybersecurity for ICT products placed on the internal market will increase[124] [125]. However, it is worth noting that the market operators of different sectors (e.g. B2B, B2C) have very diverging opinions on the soundness of a voluntary approach for certification schemes[126]. Additionally, mandatory requirements have already been placed on products for some sectors, such as medical devices through the Medical Device Regulation - Regulation (EU) 2017/745.

Concerning the lack of a common legal basis, the desk research, the feedback collected during the stakeholder engagement activities, and the conducted gap analysis have all highlighted that the existing EU legislative framework appears to be fragmented, imposing overlapping and contradictory requirements on the manufacturers of ICT products [127].

Lastly, the lack of rules for post-market surveillance of several ICT products has negative consequences in terms of consumer protection. While market surveillance is paramount for the smooth functioning of the Digital Single Market, the data collection activities pointed out that Member States do not currently have the legal basis to remove several insecure ICT products from the market. In fact, as cybersecurity is a wider concept than safety, the current market surveillance mechanisms applying to product safety legislation cannot address all the security risks related to the marketing of secure ICT products within the Digital Single Market. Additionally, in sectors where market surveillance activities take place, divergent views of market surveillance authorities represent an obstacle to cross-border activities [128]. Nevertheless, it is worth noting that the lack of rules for post-market surveillance does not concern all types of ICT products. For instance, the post-market surveillance system for medical devices has been framed by Art. 83 of Regulation (EU) 2017/745[129].

As highlighted in Figure 12, stakeholders providing responses to the targeted consultation consider the abovementioned drivers as the main root causes for the lack of secure ICT products within the EU. In fact, these root causes were the only ones scoring more than four in a five points Likert scale used in the survey[130]. The absence of a harmonised conformity assessment method across the EU Single Market represents an additional area of concern for many stakeholders[131]. As reported by some respondents, these issues are all connected by the absence of a cross-sectoral approach to the cybersecurity of ICT products in the NLF, leading to inconsistent and/or overlapping security requirements for producers.

[124] ANEC, BEUC (2018); Cybersecurity for Connected Products – Position Papers, ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018

[125] Keeping consumers secure, How to tackle cybersecurity threats through EU law, BEUC-X-2019-066 - 05/11/2019.

[126] ECSO (2017), Position Paper – Initial position on the EU cybersecurity package.

[127] Orgalim (2019), Position Paper - Building a real European Single Market for Cybersecurity: A call for a consistent approach – guiding principles

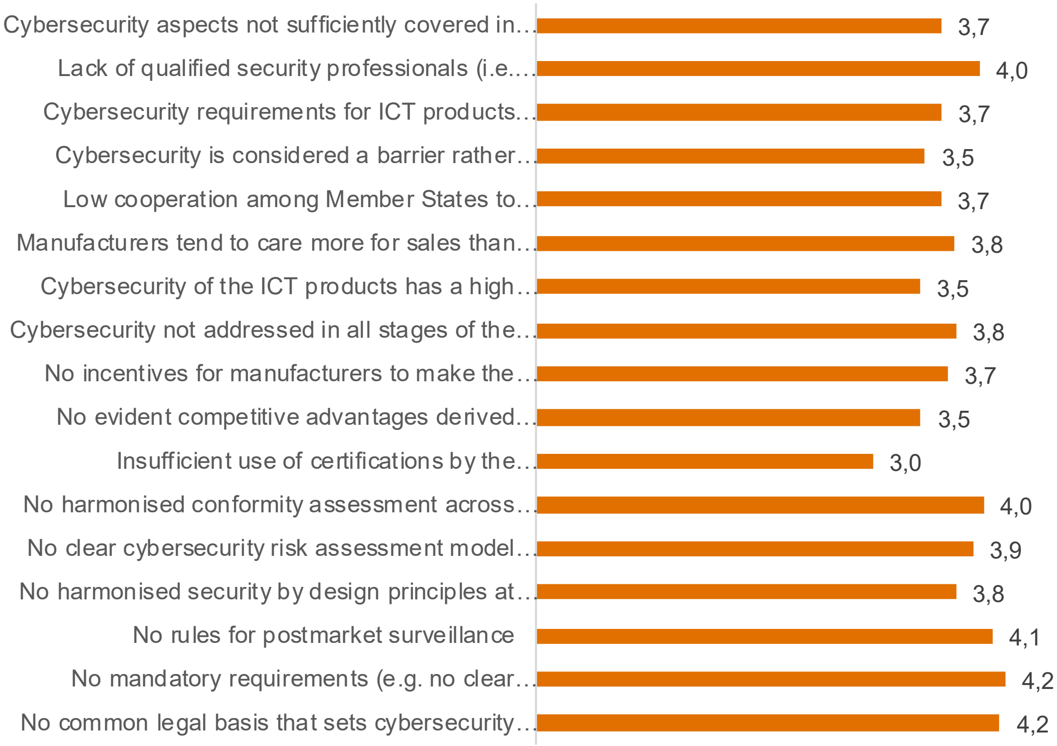
[128] European Commission (2020) Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions – Identifying and addressing barriers to the Single Market {SWD(2020) 54 final}

[129] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

[130] The problem drivers scored either 4,1 or 4,2 out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88).

[131] The problem driver scored 4 out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88).

Figure 12 Problem drivers for the inadequate security of ICT products (1-Strongly disagree; 2-Somewhat disagree; 3-Neither agree nor disagree; 4-Somewhat agree; 5-Strongly Agree)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.It is important to point out that the abovementioned problem drivers are linked to one another. Product requirements and post-market surveillance rules are mostly included in product legislation aligned with the reference provisions of the NLF[132]. As a consequence, the absence of a piece of legislation targeting ICT products, along with the proliferation of new connected devices, entails that some ICT products can be subject to provisions of different legislation (or no legislation at all).

Concerning **market failures,** the absence of a competitive advantage derived from cybersecurity, the lack of incentives for manufacturers to make the product more secure as well as the fact that cybersecurity is not always addressed at the early stages of the product lifecycle represent three relevant problem drivers.

As reported by National Competent Authorities during the data collection activities, whereas manufacturers bear certain costs when enhancing the security features to ICT products [133], consumers' willingness to pay a premium for those enhancements may be low. Furthermore, SMEs often find cybersecurity as a costly endeavour[134]. The lack of

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

[133] Information available at ; https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

[134] European Economic ans Social Committee (2018), Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.

incentives for solution providers and manufacturers to take cybersecurity into account has also been pointed out by ENISA in its report on Industry 4.0 Cybersecurity: Challenges & Recommendations[135]. The issue becomes even more evident in the Digital Single Market as there are currently no common established methods to communicate the security level of ICT products in place. Additionally, the analysis of the information collected by the Project Team suggested that cybersecurity is currently not always factored in at the early stages of the product lifecycle. Hence, it appears that the design and development as well as the deployment and configuration of secure ICT products are currently not enough considered by some manufacturers. In this regard, ENISA[136] has recommended the application of principles such as security by design and by default to address vulnerabilities throughout the lifecycle of an ICT product. Consumer associations such as BEUC and ANEC are also strong supporter of the application of the security by design principle to ICT products [137] [138].

The feedback provided during the targeted consultation highlighted that the lack of incentives for manufacturers to make their products more secure[139] as well as the reluctance to implement cybersecurity solutions in all stages of ICT product lifecycle[140] represent relevant root causes for Problem 1. Conversely, stakeholders seem to agree to a lesser extent with the absence of a competitive advantage derived from cybersecurity (see Annex V – Target Consultation Results) which represents the second lowest score among the different problem drivers. Particularly, as suggested by a stakeholder from the ICT industry, while cybersecurity as a competitive advantage is well understood by economic operators, financial costs are high and incentives remain low.

The **behavioural aspects** mainly concern the misalignment of incentives of relevant stakeholders. In this context, during the Focus Groups, it has been pointed out that the manufacturers tend to care more about sales than security. This represents a long-standing issue, correlated with the lack of competitive advantage derived from cybersecurity as well as the absence of incentives for the manufacturers to improve the security of many ICT products. In fact, the damage experienced by large corporation as a result of a cyber-attack is often negligible compared to their turnover[141] [142]. Conversely, as some academic literature has pointed out[143], incentives may arise in B2C settings (e.g. IoT) where the inclusion of security-related information encourages consumers to pay more for secure devices. The attention of producers on the sale-related aspects rather than the security one is also partially supported by the targeted consultation feedback[144].

Among **equity aspects**, the lack of qualified cybersecurity professionals represents a relevant driver for the lack of secure ICT products across the EU. Despite considering the training of enough cybersecurity professionals as an absolute priority to counter the increase of cyber-attacks, Member States (e.g. Italy, France) have pointed out the

[135] ENISA (2019) Industry 4.0 Cybersecurity: Challenges & Recommendation.

[136] ENISA (2019) Good Practices for Security of IoT - Secure Software Development Lifecycle.

[137] ANEC, BEUC (2018); Cybersecurity for Connected Products – Position Papers, ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018

[138] Keeping consumers secure, How to tackle cybersecurity threats through EU law, BEUC-X-2019-066 - 05/11/2019.

[139] The problem driver scored 3.7 out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88).

[140] The problem driver scored 3.7 out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88).

[141] Information available at : https://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

[142] ENISA (2020) Data breach – ENISA threat landscape

[143] Blythe, J.M. Johnson, S.D (2020), What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices, Crime Science volume 9, Article number: 1 (2020) Cite this article

[144] The problem driver scored 3,8 out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88).

shortage of those figures in the labour market[145]. In this regard, ENISA has reported that there are several indicators suggesting that cybersecurity remains among the most constrained sectors in the job market. As an example, while cybersecurity job postings have increased by 94% between 2013 and 2019, information technology (IT) vacancies have increased by only 30%. Additionally, cybersecurity positions have also required 20% more time to be filled than those in other IT domains[146]. The evidences resulting from the targeted consultation confirm the lack of qualified security professional as one of the main root causes of Problem 1, being considered by stakeholders as the fourth driver out of 17, related to the lack of secure ICT products across the EU [147].

Different categories of problem drivers are also at the core of the **insufficient understanding among users (e.g. citizens and companies) concerning the level of cybersecurity for ICT products (i.e. Problem 2**). For example, the lack of information provided to the consumers about the level of security of the ICT product, or the absence of cybersecurity curriculum programmes at universities dedicated to software developers. In this context, the absence of a clear definition of the requirements to ensure the appropriate (and minimum) level of security of an ICT product represents a relevant **regulatory failure**. This becomes even more problematic in the case of general-purpose devices that are likely to be used in a wide range of target environments with very different risks and where users have different levels of risk appetites [148]. The results of the targeted consultation point at the lack of a clear definition of the requirements to ensure the appropriate level of security of an ICT product as one of the main drivers to Problem 2 [149]. Additionally, during the data collection activities, some Member States (e.g. Finland) pointed out that the security requirements are imprecise as they are intended to enable a wide range of technical solutions, leaving considerable room for interpretation for the adequate implementation and requiring ongoing alignment and policy management during security audits and controls. Indeed, the absence of a clear definition of requirements depends on the fact that several ICT products do not have to fulfil any mandatory requirement at all.

Regarding the **market failures**, following the stakeholder engagement activities (i.e. Focus Groups), several stakeholders pointed out that the EU regulatory landscape does not foresee a method to communicate the security level of an ICT product to consumers. As of now, there are no effective tools to enhance transparency about the level of cybersecurity of ICT products. However, we are currently witnessing an acknowledgement of this issue by market operators. For instance, in November 2020, 11 European cybersecurity organisations started issuing the label 'Cybersecurity made in Europe' as their preferred method of communicating the cybersecurity level of their services, to differentiate European businesses from global competitors[150]. Conversely, in the views of a national competent authority answering to the targeted consultation in regards to the problem drivers for the lack of understanding about the level of security of products (see Figure 13), while methods to communicate the security level of ICT products exist (e.g. certifications), these are not used by producers.

[145] ENISA (2019), Cybersecurity Skills Development in the EU

[146] ENISA (2019), Cybersecurity Skills Development in the EU

[147] Particularly, the lack of qualified security professionals scored four out of five points in the Likert scale provided by the survey.

[148] ENISA (2019) Standardisation in Support of the Cybersecurity Certification

[149] The problem driver scored 3,7 (professional users) and 3.9 (regular users) out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88).

[150] Information available at : https://cybernews.com/news/cybersecurity-made-in-europe-label-goes-live/

Concerning the **behavioural aspects**, the data collection activities have allowed the Project Team to assess the fact that security deals on ICT products are often made in a context of asymmetric information. The presence of information asymmetries in the ICT products' markets has already been discussed in section 2.1.1 and it is recommended to refer to that part of the study for a more detailed analysis. Regarding the problem definition, it is important to point out that, while buyers cannot effectively evaluate the technology, sellers might have the incentive to place unsafe products into the market. For instance, a cable TV that is connected to the internet through a router does not respond to specific security requirements and thus is at risk of cyber-attacks. On the other hand, buyers are not often aware of these pitfalls and keep buying the products without taking into account cybersecurity aspects [151]. Furthermore, by not being able to ascertain the cybersecurity of ICT products, users often base their decision on prices, even if part of the academic literature has demonstrated that prices do not represent a good proxy for quality[152].

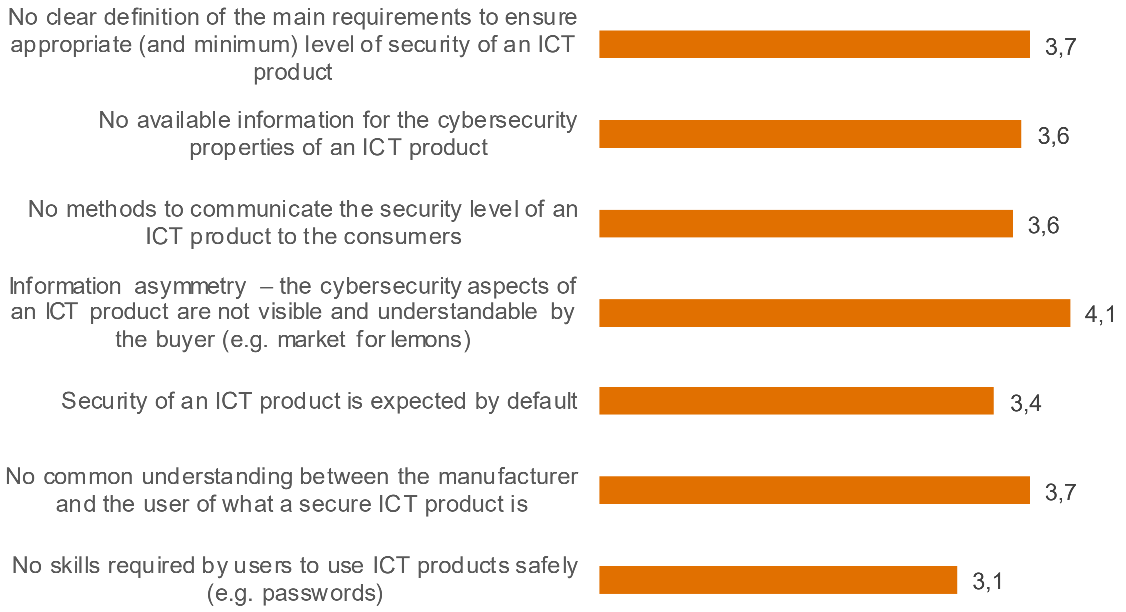
The results stemming from the targeted consultation highlighted that the presence of information asymmetries is regarded as the main root cause underlying the insufficient understanding of users concerning the level of cybersecurity of ICT products [153] (as presented in Figure 13). As reported by a national competent authority, while both professional and regular users are impacted by information asymmetries, the former generally have different (and higher) expectations with regard to the information on the cybersecurity properties of the ICT products they use. On the contrary, regular users tend to be not aware of these properties and/or not interested to be informed about these properties.

[151] European Commission, Commission Staff Working Document Impact Assessment Accompanying the Document Proposal For A Regulation Of The European Parliament And Of The Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''); SWD(2017) 500 final

[152] Some contributions: Steenkamp, J.B. (1988) The relationship between price and quality in the marketplace, De Economist volume 136, pages 491–507; Impkamp, H. (2018), Should Prices of Consumer Goods Be Better Indicators of Product Quality?, Journal of Consumer Policy, volume 41, pages 77–81.

[153] The problem driv er scored 4,1 (professional users) and 4.4 (regular users) out of 5 points of the Likert scale (N=88).

Figure 13 Problem drivers for the lack of understanding of users about the security of ICT products (1-Strongly disagree; 2-Somewhat disagree; 3-Neither agree nor disagree; 4-Somewhat agree; 5-Strongly Agree)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Among the **equity aspects**, the analysis has pointed out that users (e.g. consumers and businesses) often possess low skills to handle ICT products securely. Nowadays, we are witnessing an increasing asymmetry between the knowledge needed to perform a cyber-attack, and the skills needed to defend against it. For instance, while the spread of crime-as-a-service models has allowed individuals with no knowledge to perform cyber-attacks[154], 10% of the EU labour force possesses no digital skills and one worker out of three does not have basic digital skills, which are currently requested in the majority of the vacancies [155]. As pointed out by the results of the targeted consultation, the contribution of the lack of skills required to users on the overall persistence of Problem 2 varies greatly depending on the type of user and sector under analysis[156]. Nevertheless, it is considered to be the least relevant driver for Problem 2 both for professional and regular users[157].

[154] European Court of Auditors (2019), Challenges to effective EU cybersecurity policy – Briefing Paper

[155] European Commission (2019) Human Capital Digital Inclusion and Skills – Digital Economy and Society Index Report 2019

[156] The problem driver scored 3,1 (professional users) and 3.7 (regular users) out of 5 points of the Likert scale where 1="Strongly disagree" and 5="Strongly agree" (N=88), leading to a margin of 0,6 (second highest).

[157] The problem driver scored 3,4 out of 5 points of the Likert scale when averaging the results from professional and regular users, where 1="Strongly disagree" and 5="Strongly agree" (N=88).

2.3.4 Who are the relevant stakeholders?

The Project Team has identified the relevant stakeholders both for Problem 1 and Problem 2. Nevertheless, following the results of the data collection activities, it has not been possible to clearly draw a line between the stakeholders who are affected by the problems and those whose behaviours contributed to it. The Project Team has identified ten main categories of stakeholders:

- **Consumers**. By adapting the definition provided by Directive 2011/83/EU[158], a consumer is any natural person who acts outside his trade, business, craft or professional interests. EU consumers expect all products placed on the market to be safe and secure.
- **Developers**. A developer (or software developer, computer programmer, programmer, software coder or software engineer) is a professional that setup software and applications, writing debugs and executing the source code[159].
- **Manufacturers**. Following the definition provided by the Regulation (EC) No 765/2008, a Manufacturer Authority is "any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under his name or trademark". Manufacturers ICT products play a crucial role in ensuring that ICT products placed on market are safe and secure as they are responsible for verifying such products fulfil EU safety, health, and environmental protection requirements.
- **Digital Service Providers / Operators**. Following the definition provided by Directive (EU) 2016/1148[160], a Digital Service Provider is *"any legal person that provides a digital service"*.
- **Operators of Essential Services:** Following the definition provided by Directive (EU) 2016/1148[161], an Operator of Essential Services is *"a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)"*.
- **Network Providers**. Following the definition of operators provided by Directive 2018/1972[162], these are "*undertakings providing or authorised to provide a public electronic communications network or an associated facility"*.
- **Distributors**. Following the definition provided by Regulation (EC) No 765/2008, a distributor is "any natural or legal person in the supply chain, other than the manufacturer or the importer, who makes a product available on the market". Distributors contribute to ensure that only products compliant with EU legislation are placed on the market.
- **Market Surveillance Authority**. Following the definition provided by Regulation (EC) No 765/2008, a Market Surveillance Authority is *"an authority of a Member State responsible for carrying out market*

[158] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance

[159] Information available at : https://www.techopedia.com/definition/17095/developer

[160] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[161] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[162] Information available at : https://ec.europa.eu/digital-single-market/en/broadband-glossary

surveillance on its territory". Market surveillance authorities guarantee that non-food products marketed in the EU digital single market are not dangerous for consumers and workers. Additionally, they also verify the respect of the protection of other public interests such as the environment, security and fairness in trade.

- **National Accreditation Bodies**. Following the definition provided by Regulation (EC) No 765/2008 [163], the National Accreditation Body is the "*sole body in Member State that performs accreditation with authority derived from the State*". National Accreditation Bodies are relevant stakeholders as they define and measure products' quality in a particular area. Several accreditation bodies include quality enhancement in their field as one of the elements of their mission statement164.
- **Conformity Assessment Bodies**. Following the definition provided by Regulation (EC) No 765/2008, a Conformity Assessment Body is *"a body that performs conformity assessment activities including calibration, testing, certification and inspection"*. Conformity Assessment Bodies are important stakeholders as they perform tasks in the context of conformity assessment procedures, when a third party is required.
- **Standardisation Bodies**. Standardisation bodies are periodically updated in the list of national standardisation bodies[165] pursuant to Article 27 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council on European standardisation 2020/C 104/03. Standardisation Bodies are key stakeholders as standards are being increasingly used to address issues related to evolving technologies.

It is important to highlight that once more that this is a non-exhaustive list of stakeholders. Sub-categories of the abovementioned group of stakeholders as well as other stakeholders will be identified in section 0 when describing the lifecycle of ICT products.

2.3.5 What are the main consequences?

Among the main consequences related to Problem 1 and Problem 2, it is possible to identify economic and social ones. The Project Team did not identify any relevant direct or indirect environmental consequence in relation to the cybersecurity of ICT product. It could be argued that strengthening the cybersecurity of ICT products may result in ICT products to last longer, reducing ICT product-related waste. Nevertheless, these effects are extremely difficult to assess and could not be included in the analysis as no sound evidence has been identified. Concerning the **economic consequences**, the competitiveness of businesses may suffer from the threats related to the technology they use. Particularly, SMEs may struggle to compete in national, European and global markets.

In 2019, 12% of EU-28 enterprises with more than 10 employees, not considering the financial sector, experienced at least once problems related to an ICT security incident (e.g. unavailability of services, destruction or corruption of data, disclosure of confidential data)[166]. While large corporations are relatively more likely to suffer a cyber-attack[167],

[163] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93

[164] Information available at : https://isoupdate.com/resources/the-role-of-an-accreditation-body/#:~:text=Regarding%20the%20quality%20of%20products,improvement%20in%20their%20respective%20field.

[165] Publication of an update to the list of national standardisation bodies pursuant to Article 27 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council on European standardisation 2020/C 104/03

[166] Information available at : https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en

[167] Hiscox (2019), Hiscox Cyber Readiness Report

the damage they experience is often negligible compared to their turnover[168] [169]. Conversely, cyber-attacks may put SMEs out of business[170]. For instance, in 2014, after having suffered from a cyber-attack resulting in a loss of 56 million credit and debit card numbers and 53 million email addresses, Home Depot financial damage was estimated at USD 28 million, equal to less than 0,01 percent of the company's revenue[171]. More recently, ENISA has pointed out the divergence in cost of data breaches between SMEs and large corporations. Whereas companies with more than 25 000 employees pay on average EUR 173 per employee, the average cost for SMEs is around EUR 3 000 per employee[172]. Furthermore, SME have increasingly suffered of cyber-attacks during the last years and the trend is expected to continue in the future[173]. The above-mentioned trends are even more relevant when considering that SMEs account for 99,8% of European enterprises. As a result, according to the ECSO Barometer 2020: Cybersecurity in light of COVID-19[174], there is an increased need to help SMEs to protect their ICT infrastructures.

Following the response to the questionnaire sent to National Competent Authorities, several Member States (e.g. Czech Republic, Finland, Germany, Poland) have pointed out the undermined trust of EU citizens in commercialised products as one of the most relevant **social consequences**. In 2019, almost one individual out of five in the EU-28 declared that security concerns limited or impeded her/him from downloading software or apps, music, video files, games or other data[175]. The trend appears to be increasing over the last ten years. Cybersecurity concerns seem to affect a sub-set of ICT products, namely IoT. In this domain, security concerns deter 28% of people who do not own an IoT from buying one, making them a deterrent as strong as the price of a device[176].

Product safety and personal integrity (e.g. life, health) have also been identified as one of the most serious social consequences both during scoping interviews and the focus groups. While financial reward remains the main motivation[177], cyber-attacks are increasing capable of causing accidents that could eventually threaten human life. It has been pointed out that, in some cases, a security breach in a small component of a network can lead to disastrous consequences, particularly if such component is part of a critical infrastructure (e.g. hospitals or energy networks). A study from the Economic and Social Committee[178] has reported that, since 2000, almost one incident out of three involving critical infrastructure failure was caused by failures in other sectors.

While the implications of a cyber-attack to a critical infrastructure cannot be underestimated, relevant stakeholders have noted that security breaches in ICT products, and particularly in consumer IoT devices, can also have

[168] Information available at : https://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

[169] ENISA (2020) Data breach – ENISA threat landscape

[170] Information available at : https://www.cnbc.com/2019/10/13/cyber-attacks-cost-small-companies-200k-putting-many-out-of-business.html

[171] Information available at : https://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

[172] ENISA (2020) Data breach – ENISA threat landscape

[173] European Economic and Social Committee (2018), Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.

[174] ECSO (2020), ECSO Barometer 2020: "Cybersecurity In Light Of Covid-19 - Report on the results of surveys with ECSO members and the cybersecurity community

[175] Information available at : https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_ax/default/table?lang=en

[176] Information available at : https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

[177] Information available at : https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

[178] European Economic and Social Committee (2018), Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.

disastrous consequences and are often overlooked. In fact, the actions performed after having broken into a network are generally more important in terms of consequences then the sole fact of breaking into it. For instance, if a hacker connects to a Wi-Fi network that is not well protected, it might not represent a big issue in terms of direct damage. Nevertheless, if a user connected to the Wi-Fi happens to exchange non-encrypted emails with confidential information, the damage for the company can be enormous.

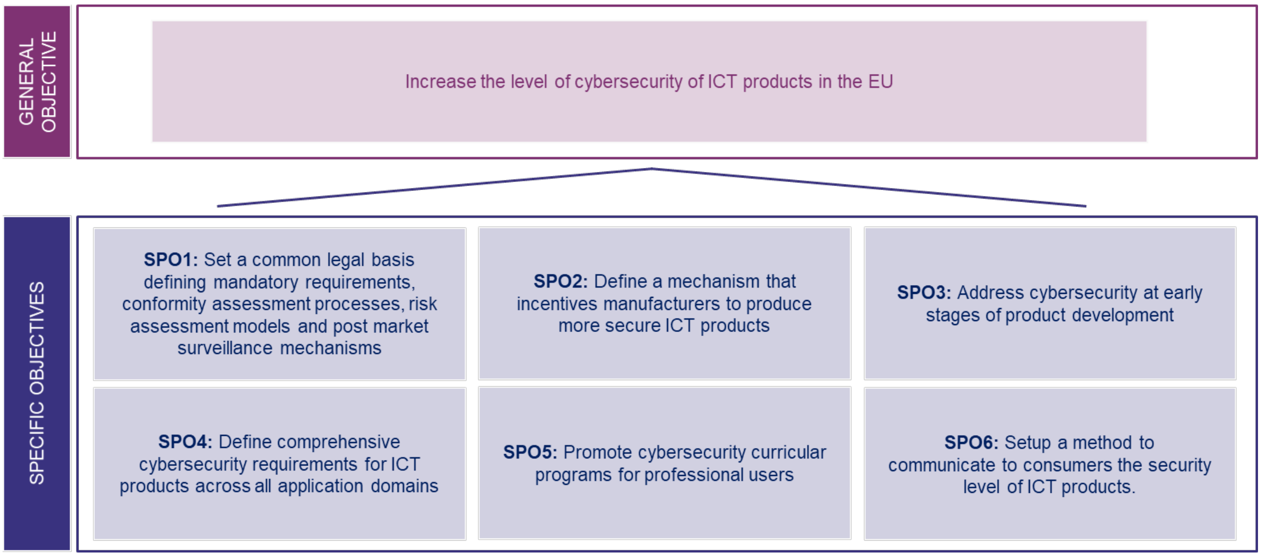
Furthermore, the lack of cybersecurity of ICT products has relevant impact on the fundamental rights (e.g. personal data, privacy and property) of citizens across the EU. For instance, insufficient levels of cybersecurity in ICT products such as surveillance cameras can expose citizens and business to the cyberattacks targeting their privacy[179]. Additionally, the upward trend in the number of ICT devices available in the EU market over the last years is expected to continue during this decade. In this regard, it is expected that more than 5.5 billion IoT devices will be active in Europe by the 2030. As these products may collect and process personal information, privacy issues should not be overlooked [180].

2.4 Policy objectives

This section reflects on the objectives for an EU policy intervention to address the issues identified in section above. This section is based on the findings resulting from the conducted interviews, focus groups and workshop, and it also includes additional feedback received during the data collection activities with relevant stakeholders in the context of the identification of the policy options. The assessment in this section follows Tool #16 from the EU Better Regulation Toolbox.

For a visual description of the preliminary objective tree see Figure 14 below.

Figure 14 Objective tree


GENERAL OBJECTIVE
Increase the level of cybersecurity of ICT products in the EU
SPECIFIC OBJECTIVES
SPO1: Set a common legal basis defining mandatory requirements, conformity assessment processes, risk assessment models and post market surveillance mechanisms
SPO2: Define a mechanism that incentives manufacturers to produce more secure ICT products
SPO3: Address cybersecurity at early stages of product development
SPO4: Define comprehensive cybersecurity requirements for ICT products across all application domains
SPO5: Promote cybersecurity curricular programs for professional users
SPO6: Setup a method to communicate to consumers the security level of ICT products.

[179] See Bloomberg (2021). Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals. Available at: https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams

[180] See Forbes (2019). Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach . Available at: https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/?sh=48a19c9f411c

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

2.4.1 What are the general and specific objectives?

The study identifies one general objective, as follows:

- To increase the level of cybersecurity of ICT products in the EU.

The general objective to be pursued through a European intervention takes into account the two problems identified in the previous section. Particularly, an increase of the level of cybersecurity of ICT products should rely upon, among others, the definition of a common legal basis and comprehensive requirements to directly address the lack of secure ICT products across the EU (Problem 1). Moreover, an intervention aimed at fostering higher level of cybersecurity of ICT products across the EU should also consider to address the insufficient understanding among users about the level of cybersecurity of ICT products (Problem 2) by i) communicating to regular users (e.g. consumers) the security of such products to allow them to better understand the cybersecurity risks associated to them and, ii) promoting cybersecurity curricular programmes among professional users (e.g. software developers).

The analysis performed allowed the Project Team to identify six specific objectives:

- SPO1: Set a common legal basis defining mandatory requirements, conformity assessment processes, risk assessment models and post market surveillance mechanisms.
- SPO2: Define a mechanism that incentives manufacturers to produce more secure ICT products.
- SPO3: Address cybersecurity at early stages of product development.
- SPO4: Define comprehensive cybersecurity requirements for ICT products across all application domains.
- SPO5: Promote cybersecurity curricular programmes for professional users.
- SPO6: Setup a method to inform consumers about the security level of ICT products.

Are there synergies or trade-offs between objectives?

The specific objectives are interrelated.

Synergies: SPO2 and SPO6 are interrelated. Manufacturers could be incentivised to produce more secure ICT products by setting up communication mechanisms (e.g. labels, notifications and alerts) that would allow them to turn into profits the higher quality of their products. Particularly, manufacturers could inform users about the high-level of cybersecurity of their ICT products. This would help uninformed consumers to distinguish between ICT products on the basis of their cybersecurity levels, taking more informed decisions depending on their individual preferences. Consequently, manufacturers applying higher cybersecurity standards could profit from their virtuous behaviours. Furthermore, SPO1 and SPO4 are also interrelated as some policy options (e.g. horizontal legislation) would entail the development of a common legal basis defining comprehensive cybersecurity requirements for ICT products across all application domains.

Trade-offs: When considering the setup of a common legal basis defining higher levels of cybersecurity of ICT products, it is important to consider that the usage of ICT products cannot be risk-free. Hence, the setup of a common legal basis and the communication of the cybersecurity levels of ICT products to consumers should be considered as complementary objectives. In case they are not pursued in parallel, trade-offs may arise. For instance, the mere setup of a common legal basis (without adequate communication measures) may let consumers believe that the usage of ICT products is risk-free and adopt risky cybersecurity behaviours (e.g. not updating their devices as recommended), ultimately limiting the benefit brought by the presence of a common legal basis.

2.4.2 What are the specific objectives that address the problems drivers?

Table 14 Links between problem drivers and policy objectives below illustrates how each driver is related to the specific policy objective and ultimately to the general objective.

Table 14 Links between problem drivers and policy objectives

Problem drivers	Specific objectives	General objectives
No mandatory requirements (e.g. no clear obligations for the manufacturer)	**SPO 1** Set a common legal basis defining mandatory requirements, certification processes, risk assessment models and post market surveillance mechanisms	Increase the level of cybersecurity of ICT products in the EU
No common legal basis that sets cybersecurity requirements for ICT products		
No rules for post-market surveillance		
No clear cybersecurity risk assessment model at EU level.		
No harmonised conformity assessment across the EU.		
No harmonised security by design principles at national level to increase the security of ICT products		
Low cooperation among Member States to define a common baseline for cybersecurity		
Insufficient use of certifications by the manufacturers		
No clear definition of the main requirements to ensure the appropriate (and minimum) level of security of an ICT product		
No evident competitive advantages derived from cybersecurity	**SPO 2** Define a mechanism that incentives manufacturers to produce more secure ICT products	
No incentives for manufactures to make the products more secure		
Cybersecurity of the ICT products has a high cost for the manufacturer		
Manufacturers tend to care more for sales than security		
Cybersecurity is considered a barrier rather than an enabler for the manufacturer		
Cybersecurity not addressed in all stages of the product lifecycle (design, development, delivery, maintenance)	**SPO 3** Address cybersecurity at early stages of product development	
Cybersecurity requirements for ICT products differ across application domains	**SPO 4** Define comprehensive cybersecurity requirements for ICT products across all application domains.	
Lack of qualified security professionals (i.e. developers)	**SPO 5** Promote cybersecurity curricular programmes for professional users	
Cybersecurity aspects not sufficiently covered in technical studies curricula.		
No skills of the users to use ICT products safely (e.g. passwords)		
No available information for the cybersecurity properties of an ICT product	**SPO 6** Setup a method to communicate to consumers the security level of ICT products	
No methods to communicate the security level of an ICT product to the consumers		
Information asymmetry – the cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons)		

Security of an ICT product isexpected by default		
No common understanding between the manufacturer and the user of what a secured ICT product is		

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

2.4.3 Are these objectives consistent with other EU policies and legislation?

This section builds on desk research performed during the analysis of the background and policy context as well as the evidences collected from the legislative gap analysis.

The Treaties

The general objectives are consistent with the articles of the Treaties.

The Charter of the Fundamental Rights of the European Union

An increased level of cybersecurity for ICT products as well as increase the understanding among users about such level of cybersecurity would be consistent with the Charter, in particular to:

- Right to liberty and security (Article 6 of the Charter), as cybersecurity of ICT products has an impact to security in general;
- Respect for private and family life (Article 7), as cyber-attacks may lead to the disclosure of private information concerning an individual and/or her/his family members;
- Protection of personal data (Article 8), which can be under threat by cyber incidents;
- Consumer protection (Article 38), since the objectives would contribute to consumer protection from cyber-attacks;
- Right to property (Article 17), since cyber-attacks can affect intellectual property;
- Right to environmental protection (Article 37) as cyber-attacks may have negative effects on the environment.

Coherence between this study and other EU interventions in the field of cybersecurity for ICT products

An EU intervention aiming at increasing the level of cybersecurity of ICT products as well as the level of understanding among uses shall build on the provisions outlined in the Cybersecurity Act (e.g. conformity assessment procedures) the last developments of the RED. The purpose, timing and scope of the RED are presented in Box 1 under section 2.1.2.

Furthermore, such intervention shall also take into account the main findings of the gap analysis. Lastly, the security and safety requirements specified in each of the 37 pieces of legislation addressing directly and/or in-directly the cybersecurity of ICT products shall also be considered in order to avoid overlaps and contradicting requirements.

2.5 Rationale for EU action

This section aims to test the respect of the legal basis and the subsidiarity principle for an EU policy intervention in the domain of cybersecurity requirements for ICT products. This section is based mostly on desk research and builds on evidences gathered during the data collection activities conducted by the Project Team. is section is guided by two research questions:

- Is the legal basis principle respected?
- Is the subsidiarity principle respected?

2.5.1 Is the legal basis principle respected?

Despite not being linked to any specific piece of legislation, a future EU policy intervention addressing the need for cybersecurity requirements of ICT products shall be based on Article 114 of the Treaty of the Functioning of the European Union (TFEU), providing legal measures to boost the overall level of cybersecurity in the EU. Particularly, Article 114 states that:

"[…] *The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market*.

[…] 3. *The Commission, in its proposals envisaged in paragraph 1 concerning health, safety, environmental protection and consumer protection, will take as a base a high level of protection, taking account in particular of any new development based on scientific facts. Within their respective powers, the European Parliament and the Council will also seek to achieve this objective*."

As discussed in the problem definition in section 2 above, the cybersecurity of ICT products is strongly related to consumer protection with implications to health, safety and environmental issues. In this regard, Article 114 of the TFEU explicitly covers safety, health, environment issues related to consumer protection.

Furthermore, following the first paragraph of Article 168 of the TFEU: "*in order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests*." By doing so, the EU shall contribute to the achievement of these objectives by adopting:

- measures pursuant to Article 114 in the context of the completion of the internal market;
- measures which support, supplement and monitor the policy pursued by the Member States.

2.5.2 Is the subsidiarity principle respected?

As discussed in section 2, cybersecurity has a strong cross-border dimension. This study has previously mentioned the impact and spill over effects related to several cybersecurity incidents. It also pointed out that cybercrimes and cyber incidents trends have increasingly become cross-border in nature. It follows that both the complexity and the extent of the cyber threats demands an EU level response. On the contrary, uncoordinated and separate responses from each Member State do not seem to represent a viable alternative to address the problem.

In fact, according to Article 4 of the TFEU, the Single Market is an area of 'shared competence' of the European Union. Particularly, following Article 26 of the same treaty, "*The Union shall adopt measures with the aim of* *establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaty*"

All in all, the objective of building an open and competitive digital single market for ICT products while ensuring high level of security for users seems difficult to achieve without a coordinated approach at the EU level. Different national requirements and/or post-market surveillance rules for the security of ICT products may result in hampering the smooth functioning of the internal market instead of addressing the issue previously identified in this study. Based on the above, an EU policy intervention in this domain respects the legality and the subsidiarity principle.

3 Identification of ICT product categories and risk profiles

This Section examines the definition of ICT products and presents a set of generic ICT products categories identified through Desk Research. Moreover, the Section offers a method to create risk profiles for each product category, in each economic sector, to enable an evaluation of risks based on impact and likelihood.

For this study, the Project Team considered as ICT Products "any products that are connected digitally, not only IoT". The study proposes an ICT product categorisation, refined from the documentation proposed by ISC, CPC, ENISA and OECD. It highlights six categories of products (such as "*End devices*", "*Software"* or "*Networks*"). Each category is additionally divided into additional subcategories for each economic sector, mapped with the relevant ISIC and CPC codes as well as with a description of the associated product**s** to provide more context.

Moreover, the Project Team developed a method to create risk profiles, applicable to all ICT products used in an economic sector. The methodology allows the development of operational scenarios as well as risk profiles by starting from the attacker perspective.

The study also offers some conclusions based on the preliminary execution of the methodology, such as the difficulty to create aggregated risk profiles per ICT product category, or per sector due to the heterogeneity of ICT products within a category or a sector. However, the results are valid as starting point for the development of policy options in the subsequent task of the project. More in general, the risk cases can also be used as base for more detailed risk profile analysis, e.g. on product level. Additionally, the methodology can be used for extended analysis in other sectors, not covered by the study.

Finally, the Section proposes paths to enhance the method used to determine the risk profiles, as well as the stakeholders which should be involved in the improvement of the method to ensure the completeness and reliability of the results.

3.1 Definition and categorisation of ICT products

3.1.1 ICT products definition

The border between ICT and non-ICT sectors is becoming increasingly blurred. As a result, there is a need for a clear definition of what is an ICT product as well as for a clear methodology to categorise them. Such a methodology will have to take into account the rise in cybersecurity threats brought by the growing market uptake of connected devices and IoT products.

To define an ICT product is not an easy task considering that the field of Information and Communication Technologies (ICTs) is a broad and fragmented domain that consists of a wide variety of infrastructure systems, devices and capabilities that were developed and operated independently from one another.[181]

[181] Manual for the Production of Statistics on the Information Economy, United Nations, 2007

In very basic terms, an ICT product can be defined as any good that has electronics or code inside and that is produced either for home/consumer or business/industrial purposes. In 2008, the OECD introduced the following definition of ICT products/goods:

- *"ICT goods must either be intended to fulfil the function of information processing and communication by electronic means, including transmission and display, or use electronic processing to detect, measure and/or record physical phenomena, or to control a physical process".*[182]

The Project Team used a Focus Group and interviews to discuss the relevance of this definition in nowadays' digital landscape, which saw the considerable expansion of the IoT. The **main findings from the expert's qualitative judgements** are summarised below:

- On the one hand, the OECD definition can be considered as representing a more bureaucratic point of view than a technical one, it **incorporates the aspects of communication, product application and electronic processing that are still relevant today**.
- On the other hand, taking into account the roll-out of the digital transformation, the definition is not fully accurate: **ICT products cannot be just reduced to physical phenomena, as they also involve digital processes**.
- The definition is too static and does not take into account the appropriation of technologies by their users. The way ICT products are used in concrete settings can drastically change over time, which can have important impacts on a product's functionalities. **Technologies are not fixed solutions to a predefined problem - they change and evolve over time and so do ICT products.**
- **Cybersecurity needs to be considered in relation to ICT products that are integrated into broader systems.**
- **The link between ICTs and IoT products is not always straightforward**. ICTs are key enabling technologies, without which the IoT could not exist[183]. However, IoT devices open up new synergies between the physical and digital worlds and represent an evolution of ICTs products.
- **ICTs is a generic term that comprises all products containing electronics, whereas IoT items are just a type of ICT products.** Specifically, concerning cybersecurity, it is important to remember that some IoT products are constrained devices (e.g. some IoT devices have no computational power, no high memory, and not very high-security demands). As a result, some manufacturers can even remove the security components to save up on the production costs.

For this study, the Project Team considers as a working definition for ICT Products "any products that are connected digitally, not only IoT". The OECD talks about "*Smart Products, i.e. products that contain code and can interconnect*". [184] These products include the associated embedded firmware and software that is essential for the primary function of the end product and is either:

[182] International Seminar on Information and Communication Technology Statistics, 19 - 21 July 2010, Seoul, Korea

[183] Measuring the Information Society Report, International Telecommunication Union, 2015

[184] Understanding the digital security of products: an in-depth analysis, OECD, 2021 - Forthcoming

- Pre-installed in a product; and
- Separately placed on the market by the hardware manufacturer or software manufacturer and downloaded to a product at a later stage. [185]

This perspective helps to capture the whole threat model, including the issues of back-end vulnerabilities (not only the device but also the web service connected to it).

3.1.2 ICT products categorisation

The difficulties in establishing a classification/categorisation/taxonomy of ICT products has been recognised for a long time. Several classifications have been developed over the years, but none of them has become a widely adopted standard.

There are several examples of ICT related classifications or taxonomies proposed in recent years:

- OECD (2003), defined using the Harmonised System, in which ICT-related technologies got subdivided into four main categories: 'Telecommunications'; 'Consumer electronics'; 'Computers and office machinery'; and 'Other ICTs'. This classification was created to "facilitate the construction of internationally comparable indicators on ICT trade and ICT production." **[186]** It was assumed from the start that the proposed categories would evolve due to the rapidly changing nature of ICT goods and services.
- ISI-OST-INPI (2005)[187], which can be considered a precursor of Schmoch's (2008) classification. In this categorisation, the 'Electrical engineering' category was subdivided into five groups instead of eight: 'Electrical machinery and apparatus'; 'Audio-visual technology'; 'Telecommunications'; 'Information technology'; and 'Semiconductor.'
- Schmoch (2008), in which all patentable technologies were subdivided into six main technology areas: 'Electrical engineering'; 'Instruments'; 'Chemistry and pharmaceuticals'; 'Process engineering and special equipment'; 'Mechanical engineering and machinery'; and 'Consumption'. In this classification, ICT technologies fall into the 'Electrical engineering' category, which is subsequently divided into: 'Electrical engineering'; 'Audiovisual technology'; 'Telecommunications'; 'Digital communications'; 'Basic communication process'; 'Computer technology'; 'IT methods for management'; and 'Semiconductors'. This classification took as a starting point the ISI-OST-INPI classification and it aimed "to provide a basic tool for the analysis of country structures and international comparisons, noted for the determination of specialisation profiles" [188].
- In the ICT classification of the Japan Patent Office (JPO)[189], ICT areas are classified into twelve groups: (1) High-speed networks; (2) Security; (3) Home electronics networks; (4) High-speed computing; (5) Simulation; (6) Large-capacity and high-speed storage; (7) Input-output; (8) Cognition and meaning understanding; (9) Human interface evaluation; (10) Software; (11) Devices; and (12) Others.

[185] Orgalim (2020), Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework, Policy Paper, p. 4

[186] Working Party on Indicators for the Information Society: A proposed classification of ICT goods, Organisation for Economic Co-operation and Development, 13 November 2003

[187] Technology classification of ISI-OST-INPI, February 2005

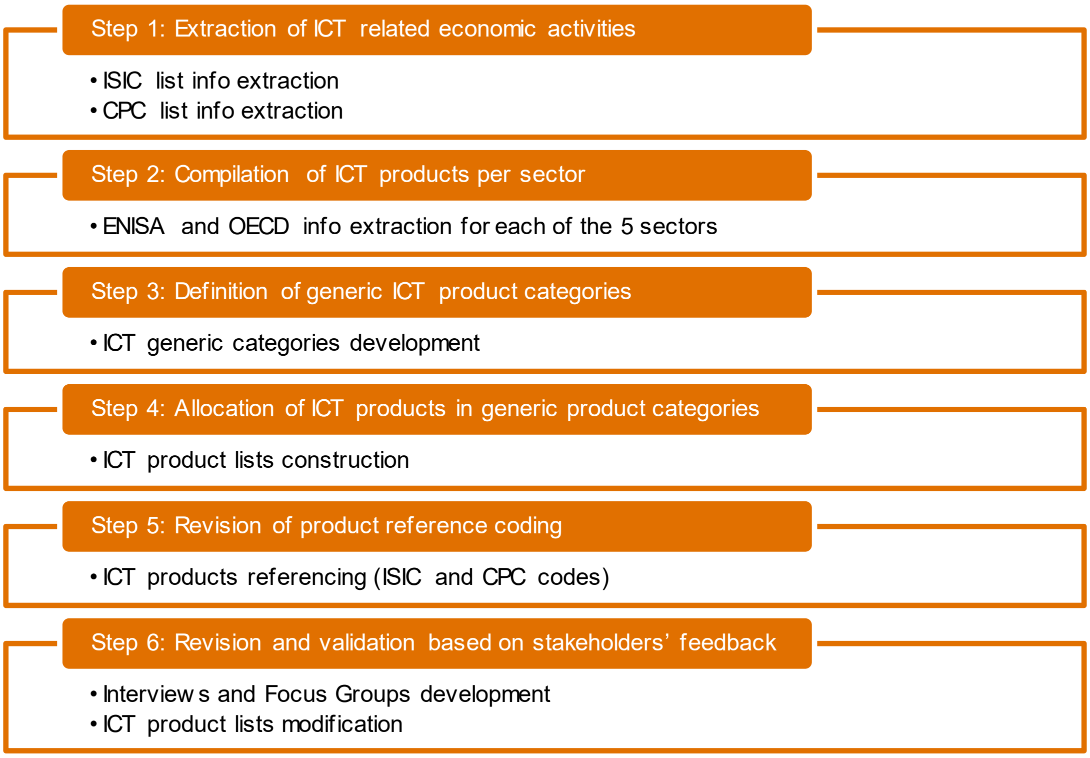
[188] Concept of a Technology Classification for Country Comparisons, World Intellectual Property Organisation (WIPO), June 2008

[189] ICT classification of the Japan Patent Office, JPO, 2017

After carrying out interviews with different international organisations, policy makers and academic experts, the conclusion reached is that the **different classifications are valid within their own terms of reference**. Each definition was created with particular objectives behind it. Although when it comes to cybersecurity, these categories are not that useful, as some products can be placed in different categories simultaneously. According to the surveyed stakeholders, the **Japanese Patent office classification is the most commonly preferred definition.**

Figure 15 presents the steps followed for the categorisation of ICT products within the respective sectors/markets.

Figure 15 ICT product list development



Step 1: Extraction of ICT related economic activities

- ISIC list info extraction
- CPC list info extraction

Step 2: Compilation of ICT products per sector

- ENISA and OECD info extraction for each of the 5 sectors

Step 3: Definition of generic ICT product categories

- ICT generic categories development

Step 4: Allocation of ICT products in generic product categories

- ICT product lists construction

Step 5: Revision of product reference coding

- ICT products referencing (ISIC and CPC codes)

Step 6: Revision and validation based on stakeholders' feedback

- Interviews and Focus Groups development
- ICT product lists modification

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Step 1. Extraction of ICT related economic activities:

ICT economic activities were listed based on the information from the ISIC list of Economic Activities [190] and the CPC (Central Product Classification) list[191].

Step 2. Compilation of ICT products in each sector:

The following sources were used to develop the first list of ICT products for each of the five sectors covered by the study (Smart Manufacturing, Finance, Energy, Transport and Smart Home)[192]. The Project Team, in agreement with

[190] International Standard Industrial Classification of All Economic Activities: Revision 4, United Nations, New York, 2008

[191] Central Product Classification (CPC): Version 2.1, United Nations, New York, 2015

[192] The five sectors covered by the study were selected in agreement with DG CNECT.

DG CNECT, has selected these indicative product categories and sectors on the basis of their good representativeness with regards to the cybersecurity of ICT products and to prepare work related to policy options definition especially on sector-specific policy options. Some sectors considered to be included at the beginning of the project were finally left out. Among them, eHealth was left out due to the existence of legislation around medical devices [193]. Other sectors such as Smart Cities (partly covered by Energy and Transport) were left out to limit the scope of the project.

- **Smart Manufacturing:** the ENISA study about cybersecurity in Smart Manufacturing [194].
- **Finance:** the OECD's report about Financial Markets digitalisation[195] and the ICTC report about ICT in the financial sector[196.].
- **Energy:** the ENISA's reports about cybersecurity in Smart Grids [197], the MDPI's report about Internet of Things and the Energy Sector 198 and the OECD report about ICT applications in Smart Grids [199].
- **Transport:** the ENISA's reports about cybersecurity in Smart Airports [200] and Smart Ports [201].
- **Smart Home:** the ENISA study about cybersecurity in Smart Homes [202].

For each sector, the expected benefits for the incorporation of ICT products were taken into account. Desk research identified evidence about how the presence of ICTs affects the respective sector.

- **Smart Manufacturing**: Maximise capabilities such as cost, delivery, flexibility and quality by using advanced technologies that promote rapid flow and widespread use of digital information, according to the ENISA's 2018 report about Good Practices for Security in the context of Smart Manufacturing [203].
- **Finance:** Secure transactions, global financial opportunities and internal security, according to ENISA's 2014 report about Network and Information Security in Finance Sector [204].
- **Energy**: Consumption reduction, supply and demand management and efficiency, according to World Energy Council's 2018 report about the role of ICT in Energy Efficiency Management[205].
- **Transport:** Improved security and efficiency in activities related to cargo, improved security and efficiency in activities related to passengers and improved security and efficiency in activities related to vehicles, according to ENISA's 2019 report about Ports' cybersecurity, ENISA's 2016 report about Smart Airports.
- **Smart Home:** Security, saving and leisure and comfort, according to ENISA's 2015 report about Security in Smart Home Environments.

[193] Information available at: https://ec.europa.eu/health/md_sector/overview_en

[194] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, November 2018

[195] Financial Markets, Insurance and Private Pensions: Digitalisation and Finance, OECD, 2018

[196] ICT in the financial services sector: Assessing the Human Resource Needs, ICTC, June 2012

[197] Appropriate security measures for smart grids, ENISA, December 2012

[198] Internet of Things (IoT) and the Energy Sector, Naser Hossein Motlagh, Mahsa Mohammadrezaei and Julian Hunt and Behnam Zaker, January 2020

[199] ICT Applications for the Smart Grid, OECD, January 2012

[200] Securing Smart Airports, ENISA, December 2016

[201] Port Cybersecurity - Good practices for cybersecurity in the maritime sector, ENISA, November 2019

[202] Threat Landscape for Smart Home and Media Convergence, ENISA, February 2015

[203] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, 2018

[204] Network and Information Security in the Finance Sector, ENISA, December 2014

[205] The Role of ICT in Energy Efficiency Management, World Energy Council, 2018

Step 3. Definition of generic ICT product categories:

Based on the ENISA´s ICT generic classification categories, a series of six categories of ICT products was developed: end devices; networks; servers and systems; security; software; and programs for decision support.

Scope limitation*:* Although several sources considered ICT services as ICT assets, the study was limited to analysing products (including hardware, software and back-end servers). Furthermore, although Information was identified as a potential category of ICT products, it was not included in the final lists as it is not considered an ICT product from a cybersecurity perspective. Several reports mentioned cloud services as ICT products. Even so, to limit the scope, they were not contemplated for this project.

Step 4. Allocation of ICT products in generic product categories:

For each sector, the Project Team allocated the identified ICT products into the developed generic categories.

- **Smart Manufacturing:** It was divided into End Devices, Networks, Programs for decision support, Security, Software and Servers & Systems;
- **Finance:** It was divided into End Devices, Networks, Programs for decision support, Security and Software;
- **Energy**: It was divided into End Devices, Networks, Programs for decision support, Security, Software and Servers & Systems;
- **Transport:** It was divided into End Devices, Networks, Security, Software and Servers & Systems;
- **Smart Home:** It was divided into End Devices, Networks, Security and Software.

Three sectors (Smart Manufacturing, Finance and Smart Home) allowed for the development of a general classification of ICT products based on the documental review. However, both the Energy and the Transport sectors entail a large variety of ICT products that were not possible to fully map within the scope of the project. Consequently, the scope of both the Energy and the Transport sector was narrowed down.

Scope limitation: For the energy sector Oil and Gas were not considered. The lists of products refer only to the electrical distribution network (Smart Grids). For the transport sector, products related to individual transport were not considered, limiting the lists to ports and airports. The railway sector was not considered either, although ENISA's report on the Smart Cities sector[206] addresses metro and light rails. Traffic regulation is also out of scope of our study, although covered by the same report from ENISA.

Step 5. Revision of product reference coding

With the categorisation made, the lists were revised to reference all ICT products with their corresponding ISIC codes and CPC codes.

Step 6. Revision and validation based on stakeholders' feedback:

Once the preliminary lists were built based on desk research, the list drafted by the Project Team were tested, validated and updated based on the feedback from a series of the interviews and Focus Groups carried out with representatives of different international organisations, policy makers and academic experts.

[206] Information available at: https://www.enisa.europa.eu/publications/smart-cities-architecture-model

The steps described above resulted in the lists of ICT products classified by common categories and sectors. It should be noted that, due to the limitations in terms of project scope, budget and time frame, the product lists produced are by no means to be considered exhaustive. Feedback from the Second Workshop with stakeholders indicates that future research should map existing certification schemes, to ensure consistencies with the categories of ICT products and categories that are already used or existing on the field. The full lists are listed in Annex II – ICT Product List. Table 15 below provides an overview of the products that are included in each of the six ICT product categories for the different sectors:

Table 15 Summary of ICT products per category and sector

Sector Category	Smart Manufacturing	Finance	Energy (Smart grid)	Transport (Ports and airports)	Smart Home
End devices	Sensors and cameras; Safety instruments; Actuators; Mobile devices; Smart robots and automated guided vehicles.	Smart cards; ATMs; Sensors and cameras; Mobile devices	Sensors and sensor network; Smart meters; End user interface; Mobile devices	Related to facility specific lay-out; Related to vehicles moving; Related to vehicles loading and unloading; Related to temporary storage; Related to hinterland connectivity; Mobile devices	Sensors and cameras (incl. Smart toys); Mobile devices; Robotics; Home appliance; Actuators; Other systems; Smart Speakers
Software	Code; OS; Apps; Antivirus; Firmware	Online banking apps and webs; Electronic commerce apps and webs; Cryptocurrency; Websites and online courses; Budget; retirement planning and self-commitment tools; Digital platforms; Direct trading and investment platforms; Social trading platforms; Robo-advice platforms; Risk app; Antivirus; Firmware	Code; OS; Apps; Antivirus; Firmware	Code; OS; Apps; Antivirus; Firmware	Code; OS; Apps; Antivirus; Firmware
Networks	Routers; IoT Gateways; Switches; Wireless Access Points; Firewall; Protocols; Power supply.	Routers; IoT Gateways; Switches; Wireless Access Points; Firewall; Protocols; Online adds; Regular communications; Customer support	Routers; IoT Gateways; Switches; Wireless Access Points; Firewall; Protocols	Radio; Protocols; Switches; Routers; Hubs	Telephone; Internet connection; Cable connection; Networking components; Tags and markers
Security	SIEM; IDS/IPS	Data encryption; Biometric technology; Data analytics; Distributed Ledger Technology (DLT)	SIEM; IDS/IPS	Detection systems; Emergency communication systems; Access control; Traffic monitoring; Surveillance & inspection; Evacuation; Identification & authentication; Alerting	Windows and door control; Alarm system; Access control
Servers & Systems	Historians; App servers; Database servers; Enterprise op. systems; Manufacturing op. systems; Industrial Control System (PLCs, RTUs, DCS, SCADA); End user interface	NA	Historians; App servers; Database servers; PLCs; SCADA; RTUs	ICS; ICS Communications networks & components; Community system; Cargo system; Corporate systems; Terminal Operations Management Systems; Traffic service; Servers	NA
Programs for decision support	AI and Machine learning	Algorithms; AI; Facial recognition; Health AI	Algorithms; AI	NA	NA

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Note: Non-exhaustive list. Cells marked with NA (Not Applicable) mean that information is missing for the combination of sector and product category.

3.2 Risk profiles development

3.2.1 Risk assessment

Risk assessment methodologies greatly differ across the Member States considering there is not any European-wide framework. Consequently, this section develops a risk assessment methodology at the industry level so it can be applied across European borders, regardless of the methodology selected at the national level. The methodology developed in sub-section 4.2.1 will be used to develop risk profiles in the next sub-section (0).

Table 16 presents the five key characteristics that were defined to review existing Risk Assessment methodologies and to select the most suited one for the purpose of this study[207].

Table 16 Selection criteria for Risk Assessment Methodologies

N°	Criterion	Description
1	Easy to understand and perform	The method must be clear and concise in its description. Complex methods are restricted to experts and difficult to understand for layman. In addition, a too complex framework is more disposed to mistakes during application
2	Widely applicable	The method is applied in the same way and independently to each sector. The more adaptable the method, the more precise its application is in each specific evaluation case.
3	Quantitative and qualitative method	Quantitative methods give objective results while qualitative methods, although more subjective, may give more accurate and reasoned/explained results. As both methods have their own merits, frameworks combining both approaches are the most impactful and versatile.
4	Appropriate for large organisations	Methods that can be applied to large and small case studies (e.g. SMEs and large corporations) are favoured over size-specific methodologies.
5	Risk assessment lifecycle	The risk management process should be applied as early as possible in the project life cycle, so that risks are identified, assessed, and appropriate responses developed before moving to execution.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Five risk assessment methodologies were identified as the most suited for the list of ICT product developed in sub-task 2.1. These methods were screened using the five selection criteria detailed right above.

- **CRAMM**. Especially efficient for large organisations — either governmental or private —, the CRAMM method was originally developed for the British government by the CCTA (Central Communication and Telecommunication Agency), now renamed Office of Government Commerce (OGC). Difficult to use without the related tool, the CRAMM method is now widely used outside of the UK[208].
- **EBIOS RM.** Originally developed by the French government, the EBIOS method was published by the National Cybersecurity Agency of France (ANSSI) but has been adopted globally. Methodology designed to assess and address digital risks, the EBIOS method can be used for both governmental and private bodies. The method includes a set of guidelines (and an open source software) for risk assessment that are monitored and updated by a forum of international experts (Club Ebios). This methodology is compliant

[207] Risk Assessment of China's Overseas Oil Refining Investment Using a Fuzzy-Grey Comprehensive Evaluation Method, Hui Li, Kangyin Dong, Hongdian Jiang, Renjin Sun, Xiaoyue Guo and Yiqiao Fan, 28 April 2017

[208] Information avaialble at : https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

with major IT security standards and produces best practices as well as application documents targeted to end-users in various contexts.

EBIOS RM gives risk managers a consistent and high-level approach to risks. It helps them acquire a global and coherent vision, useful to support decision-making by top managers on global projects (business continuity plan, security master plan, security policy), as well as on more specific systems (electronic messaging, nomadic networks or web sites for instance). EBIOS clarifies the dialogue between the project owner and project manager on security issues. This contributes to relevant communication with security stakeholders and spreads security awareness. EBIOS turns out to be a flexible tool. It may produce a wide range of deliverables (SSRS, security target, protection profile, action plan, etc). Local standard bases (e.g. German IT Grundschutz) are easily added on to its internal knowledge bases (attack methods, entities, vulnerabilities) and catalogues of best practices (EBIOS best practices, ISO/IEC IS 17799). [209]

- In September 2012, **NIST** released a Guide for conducting Risk Assessments (NIST 2012). The NIST guide highlights that risk-assessments should be consistently applied throughout the entire organisation being assessed. Furthermore, the guide insists on the importance of giving organisations maximum flexibility in applying their provided guidelines. Indeed, there are no clear requirements for risk analysis that could be considered valid for all organisations. The NIST guide also details the important limitations to the conclusions that can be drawn from risk analyses. These limitations include: lack of data quality to build on, lack of accuracy in the measurement instrument, the subjective nature of many risk assessment tools and data trustworthiness. In addition, the results from risk analyses have to be interpreted, which can lead to erroneous conclusions. Finally, organisations must be vigilant that the quality of a risk analysis will depend of the skills and capabilities of the individuals or groups conducting the assessment.[210]
- The **UK's Technical Risk Assessment (HMG) IA Standard No. 1** (issue 3.51) from 2009 (CESG & Cabinet Office 2009) is a component of the UK government's policy framework and is intended for the public sector. It provides a framework to identify, assess and determine the level of risk of an ICT system. This guidance is made clearer through the provision of concrete examples and is especially helpful to understand the risk analysis lifecycle. (In a conventional risk assessment, the threats are identified, then who or what would be affected and how. Finally, the risk is evaluated and measures are proposed. In addition to that, the results are evaluated after applying the measures and, if necessary, the method is updated.).[211]
- **The Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE)**. The OCTAVE approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a "self-directed approach", meaning that people from an organisation assume responsibility for setting the organisation's security strategy. The OCTAVE-S approach is an alternate version tailored to the limited means and specific constraints faced by small organisations (less than 100 people). Implementing this method only require a small interdisciplinary team of 3 to 5 people. However, for this method to be efficient,

[209] Information available at : https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

[210] Guide for Conducting Risk Assessments, National Institute of Standards and Technology, September 2012

[211] HMG IA Standard No. 1, Technical Risk Assessment, National Technical Authority for Information Assurance, October 2009

the team members must be highly familiar with all of the organisation's business and security processes. The team is in charge of the risk analysis, which includes to gather and analyse information, to produce a protection strategy and mitigation plans based on the organisation's unique operational security risks.[212]

Table 17 below provides a comparative overview of the five identified Risk Assessment Methodologies.

Table 17 Comparative analysis of Risk Assessment Methodologies

Strengths Methods	Easy to understand and perform	Appropriate for large organisations	Widely applicable	Quantitative and qualitative method	Risk assessment lifecycle
CRAMM		✓	✓		
EBIOS RM	✓	✓	✓	✓	
NIST 2012	✓		✓	✓	
HMG IA Standard No. 1		✓	✓		✓
OCTAVE	✓		✓		✓

Source: Study on the need of Cybersecurity requirements for ICT products (2021)

Applicable to large organisations across different industries, the EBIOS method is also less prone to errors and provides the most accurate method for risk assessment. Consequently, the **EBIOS method was selected as the most suited for the development of generic ICT product risk cases.**

The EBIOS Risk Manager (EBIOS RM) provides a toolbox that can be adapted to a project's objective. EBIOS RM is compatible with the reference standards for both risk management and cybersecurity. The method enables to carry out a digital risk assessment, to identify mitigation measures as well as an acceptable level of risk. It also works as a process for continuous improvement of cybersecurity within an organisation,

The EBIOS RM method[213] is an iterative approach based on five steps: (1) Scoping; (2) Defining risk origins & Target objectives; (3) Building strategic scenarios; (4) Definition of operational scenarios; (5) Identifying treatment for risks. The fifth step is left aside as this study is interested in the development of a risk assessment methodology— which is addressed in the four initial steps. For this study, the method was used to create risk scenarios or risk cases related to ICT product categories. The work was conducted based on desk research complemented with expert opinions achieved from interviews and focus groups.

The following studies were the main source leveraged for the development of risk cases for our five economic sectors:

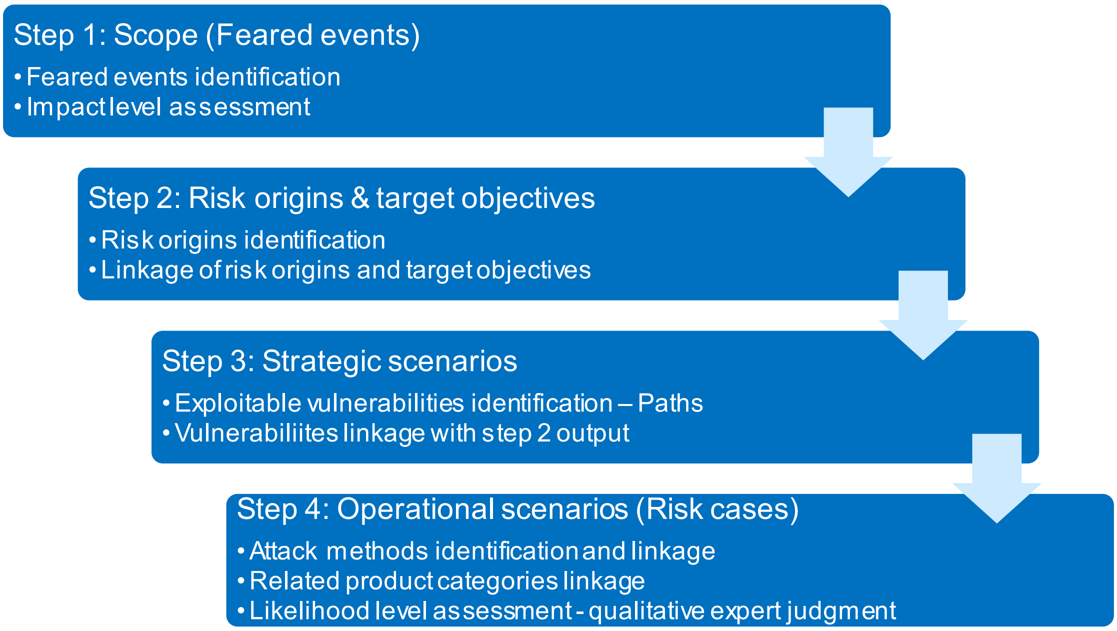
[212] Information available at : https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

[213] Information available at : https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

- ENISA's "Good Practices for Security of Internet of Things in the context of Smart Manufacturing" [214] report;
- ENISA's "Threat Landscape Report 2018"[215] report;
- ENISA's "Security of Mobile Payments and Digital Wallets"[216] report;
- ENISA's "Communication network interdependencies in smart grids"[217] report;
- ENISA's "Good practices for cybersecurity in the maritime sector"[218] report;
- ENISA's "Securing Smart Airports"[219] report;
- ENISA's "Threat Landscape for Smart Home and Media Convergence"[220] report;
- ENISA's "Security and Resilience of Smart Home Environments"[221] report; and
- Faculty of Environment and Technology, Frenchay, Bristol "Cyber Security Challenges within the Connected Home Ecosystem Futures"[222].

The development for the **Smart Manufacturing sector is presented in** Figure 16 **below, as an example,** while results for the other sectors are included in Annex III – Risk profiles tables.

Figure 16. EBIOS risk manager steps - adapted to the purposes of the study


Step 1: Scope (Feared events)
• Feared events identification
• Impact level assessment
Step 2: Risk origins & target objectives
• Risk origins identification
• Linkage of risk origins and target objectives
Step 3: Strategic scenarios
• Exploitable vulnerabilities identification – Paths
• Vulnerabiliites linkage with step 2 output
Step 4: Operational scenarios (Risk cases)
• Attack methods identification and linkage
• Related product categories linkage
• Likelihood level assessment - qualitative expert judgment

Source: Study on the need of Cybersecurity requirements for ICT products (2021)

[214] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, November 2018

[215] ENISA Threat Landscape Report 2018, ENISA, January 2019

[216] Security of Mobile Payments and Digital Wallets, ENISA, December 2016

[217] Communication network interdependencies in smart grids, ENISA, January 2016

[218] Good practices for cybersecurity in the maritime sector, ENISA, November 2019

[219] Securing Smart Airports, ENISA, December 2016

[220] Threat Landscape for Smart Home and Media Convergence, ENISA, February 2015

[221] Security and Resilience of Smart Home Environments, ENISA, December 2015

[222] Cyber Security Challenges within the Connected Home Ecosystem Futures, Abdullahi Arabo, 2015

Step 1 (Scope definition)

Original EBIOS method: The first step defines and scopes the studied object, the stakeholders to involve as well as the timeframe. During this step, (1) the missions, business assets and supporting assets related to the studied object are listed; (2) the feared events associated with the business assets are listed and the severity of these events' impacts is assessed; (3) the security baseline and the differential are defined

Adapted method: In subtask 2.2, security baseline is considered to be out of scope, as the Project Team has applied the method in a generic manner across product categories. Referring to the first part, the product categories have been identified in the previous subtask 2.1. An important limitation of this method adaptation is the focus on the generation of risk scenarios or risk cases for generic product categories. The intended use of the product is therefore not considered in detail but only at a macro level, through the assessment of the same product categories in different sectors.

Outputs: identification of feared events and their level of severity.

The severity of the feared events is measured on a 3-level scale, distinguishing between low, medium or high severity:

- *Level 1 – Low severity*: Degradation in the performance of the activity with no impact on the safety of persons and assets. The company will overcome the situation despite a few difficulties (operation in degraded mode).
- *Level 2 – Medium severity*: High degradation in the performance of the activity, with possible significant impacts on the safety of persons and assets. The company will overcome the situation with serious difficulties (operation in a highly degraded mode).
- *Level 3 – High severity*: Incapacity for the company to ensure all or a portion of its activity, with possible serious impacts on the safety of persons and assets.

The same methodology was used for all sectors and is illustrated below with the example of Smart Manufacturing.

The main source for the identification of feared events in Smart Manufacturing was the ENISA's report on "Good Practices for Security of Internet of Things in the context of Smart Manufacturing". The report analyses and describes different cyber-attack scenarios and their impact on smart manufacturing. In addition, experts were interviewed about how critical they perceive each impact to be (not important, medium or high importance). These interviews were the main source to define the list of feared events and score their severity (see Table 18).

Results from desktop-research and expert interviews confirmed that human loss and injuries is the most feared scenario, followed by theft of sensitive information — including both personal data and classified business/production data. This is because information theft can compromise an entire business, either immediately or in an unforeseeable future when the stolen data will be used by the thieves.

Table 18 Feared events list – Smart manufacturing (example)

Feared events	Severity
Manipulation or loss of control, damage of the batch/product and infrastructure	2/3
Production processes affection or shutdown	2/3
Human injuries or death	3/3
Fraud and money steal	2/3

Feared events	Severity
Sensitive and critical data theft	3/3
Systems damages or worst, destruction	2/3

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Step 2 (Risk origins and target objectives)

Original EBIOS method: In the second step, the risk origins (RO) and their high-level targets, called target objectives (TO), are identified and characterised. The results are formalised in a mapping of the risk origins.

***Adapted method**:* In subtask 2.2, during this step **risk origins and their targets are identified**.

Outputs: identification of the list of RO/TO pairs.

The risk origins are linked to a list of four groups of potential attackers (cybercriminals, hacktivists, state-sponsored attackers and insider-attackers). These attackers' and their targets (which corresponds to the feared events identified in step one) are listed in the Table 19 below[223].

Table 19 Risk origins/target objectives list – Smart manufacturing (example)

Risk origins (attacker)	Target objectives	Description/details
Cybercriminals	Fraud and money steal Sensitive and critical data theft	Cybercriminals are individuals or group of people who use technologies to steal sensitive corporate information, personal data or money. Data theft are typically done to either sale to competitor or for ransom. They are currently the most prominent and active type of attacker.
Hacktivists	Human injuries or death Sensitive and critical data theft Systems damages or worst, destruction	Hacktivists are individuals or groups of hackers who carry out malicious activities to promote a political agenda, religious beliefs, or a social ideology. Hacktivists have ideological rather than economic objectives, and are therefore more interested in inflicting damages to equipment or in causing interruption of services. Some hacktivist can also be interested in fame or in causing injuries or even death in the case of terrorist cyberattacks.
State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure Production processes affection or shutdown Sensitive and critical data theft Systems damages or worst, destruction	State-sponsored attackers' objectives are aligned with their country's interests, which can be political, commercial or military — or even a mixture of those. This type of attackers is very challenging for cyber defence. As they enjoy state-support, these groups are typically highly skilled individuals with vast resources at their disposal. In addition, the strategy they follow is not time-oriented and focus on identifying systems' vulnerabilities that can be exploited before the release of patches. These groups aim at achieving maximum damages to their target (this does not have to include human losses). Although it is the most potent and feared attacker, it is also the least common.
Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure Fraud and money steal Systems damages or worst, destruction	Internal threats usually come from employees or former employees, but they may also come from third parties, which includes contractors, temporary workers or customers. Insider attack may involve an employee or customer seeking profit or revenge, or a contracted company.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Step 3 (Strategic scenarios)

***Original EBIOS method**:* The third step consists in a mapping of the digital threats that exists in the digital ecosystem, related to the business assets listed in the first step. This mapping then allows to develop high-level risk scenarios — also referred to as strategic scenarios. Looking at the attack's origin, the scenarios identify and detail

[223] Information available at : https://www.javatpoint.com/types-of-cyber-attackers

the attackers' likely path to reach their targets. This step allows to identify the measures necessary to secure the digital ecosystem.

Adapted method: The identification of threats and the development of strategic scenarios are done. However, the definition of security measures is left aside as it falls outside the scope of the task.

Outputs: identification of exploitable vulnerabilities and paths taken by attackers identified in step 2.

Table 20 below summarises the findings of the previous steps, bringing together the objectives, the risk origin/attackers and the attack path. These paths typically correspond to the network's vulnerabilities that can be easily exploited by the attacker. For example, for information theft, an insecure network is the easiest way to access and acquire exchanged information.

Table 20 Paths/Exploitable vulnerabilities list – Smart manufacturing (example)

Risk origins	Target objectives	Paths
Cybercriminals	Fraud and money steal	Insecure Network Insufficient Privacy Protection
	Sensitive and critical data theft	Lack of Secure Update Mechanism Insufficient Privacy Protection Insecure Data storage
Hacktivists	Human injuries or death	Use of insecure or outdated components Lack of Physical Hardening
	Sensitive and critical data theft	Insecure Network Insufficient Privacy Protection Insecure Data storage
	Systems damages or worst, destruction	Lack of Secure Update Mechanism Use of insecure or outdated components Lack of Physical Hardening
State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Secure Update Mechanism Use of insecure or outdated components Lack of Physical Hardening
	Production processes affection or shutdown	Use of insecure or outdated components Lack of Physical Hardening
	Sensitive and critical data theft	Insecure Network Insufficient Privacy Protection Insecure Data storage
	Systems damages or worst, destruction	Lack of Secure Update Mechanism Use of insecure or outdated components Lack of Physical Hardening
Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components Lack of Physical Hardening
	Fraud and money steal	Weak or guessable passwords Insufficient Privacy Protection
	Systems damages or worst, destruction	Use of insecure or outdated components Lack of Physical Hardening

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Step 4 (Operational scenarios):

Original EBIOS method: The fourth step is to develop technical/operational scenarios and assess their likelihood. These scenarios include the methods of attack that are likely to be used by the attackers and the assets related to the attack scenario.

Adapted method: no changes.

A 3-level qualitative scale is used to score the different scenarios' likelihood.

- *Level 1: Rather unlikely (low likelihood)*. The attacker has little chance of reaching its objective by one of the considered methods of attack.
- *Level 2: Likely (significant likelihood)*. The attacker could reach its target objective by one of the considered methods of attack.
- *Level 3: Very likely (high likelihood)*. The attacker will probably reach its target objective by one of the considered methods of attack.

Outputs: Identification of a list of operational scenarios or risk cases.

The four successive steps that have been described are brought together and summarised in Table 21. The table provides the tools (attack method) that the attacker (risk origin) will use to exploit a vulnerability (paths) and achieve its objective. For instance, an attacker could use a MiTM (man-in-the-middle) attack to penetrate an insecure network in order to steal information.

Once the scenario has been built, it is linked with the product categories of subtask 2.1 that may be involved in such attack. Then, for each of these scenarios (risk cases), the likelihood that the attack will be successful is evaluated.

The impact for each type of attack is directly linked to the severity of the objective. On the other hand, the type of attacker, tools, or paths taken do not affect the target's severity. For instance, human injuries or death will always be considered the maximum impact, regardless of how the attack was conducted.

Conversely to the level of severity, **likelihood has to be assessed considering all parameters**. Indeed, likelihood indicates the probability for an attack to be successful, given a specific attacker type, objective, path and tool. **Likelihood levels have been assigned based on qualitative opinions collected during focus groups and/or interviews with cybersecurity experts active in the studied sectors**. As the number of consulted experts was limited, the provided likelihood levels are mainly intended as indications rather than objective assessment.

Table 21 Risk cases list – Smart manufacturing (example)

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Cyber-criminals	Fraud and money steal	Insecure Network	Malware, MiTM attack	Networks	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	2/3
	Sensitive and critical data theft	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
		Insecure Data storage	Manipulation of info, data abuse	End devices, Security	3/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	1/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3
	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	Networks, Programs for decision support	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	2/3
		Insecure Data storage	Manipulation of info, data abuse	End devices, Security	2/3
	Systems damages or worst, destruction	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	2/3
		Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	2/3
State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	1/3
		Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	1/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3
	Production processes affection or shutdown	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	2/3
	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	Networks, Programs for decision support	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
		Insecure Data storage	Manipulation of info, data abuse	End devices, Security	3/3
	Systems damages or worst, destruction	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	2/3
		Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3
Insider attacker	Manipulation or loss of control,	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
	damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	2/3
	Fraud and money steal	Weak or guessable passwords	Manipulation of info, data abuse	End devices, Security	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

3.2.2 Risk profiles

The risk assessment method developed in the previous section allows the construction of a series of cyberattack cases in a structured way. The resulting lists detail the attackers, their objectives, their tools and attack paths. Additionally, the final list provides an assessment of the attacks' likelihood of success.

The three following steps allowed to develop risk profiles linking the categories of product (from subtask 2.1) **to the different attack cases.**

- Reordering the attack cases by type of ICT product categories for each sector separately and see how many of the risk cases each category is involved;
- Indicating, for each case, both the level of likelihood and the level of impact; and
- Development of a summary table to illustrate how critical each product category is for each sector (Finance, Smart manufacturing, Smart home, Energy-Smart grid and Transport-Ports & Airports).

To illustrate this methodology, the example of "End Device" for the Smart Manufacturing sector is presented below (see Table 22). The complete table as well as the table for the other sectors are provided in Annex III – Risk profiles tables.

Reminder: The impact level is only correlated to the objective's severity (e.g. killing human beings) while the level of likelihood is assessed considering all parameters (see Annex III – Risk profiles tables). Likelihood levels were assigned based on opinions collected during focus groups and/or interviews with cybersecurity experts active in the sectors under scrutiny.

Table 22 Product categories risk cases – Smart manufacturing (example)

Product category	Risk cases					
	Risk origin	Target objective	Path	Attack method	Impact	Likelihood
End devices (Sensors and cameras, Safety instruments, Actuators, Mobile devices, Smart robots and automated guided vehicles)	Cyber-criminals	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	3/3
	Cyber-criminals	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	3/3
	State-Sponsored attackers	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	3/3
	State-Sponsored attackers	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	3/3
	Hacktivists	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Hacktivists	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	2/3
	Insider attacker	Fraud and money steal	Weak or guessable passwords	Manipulation of info, data abuse	2/3	3/3
	Insider attacker	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	3/3
	Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	1/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3
	Cyber-criminals	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Production processes affection or shutdown	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Product category	Risk cases					
	Risk origin	Target objective	Path	Attack method	Impact	Likelihood
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Production processes affection or shutdown	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors’ own elaboration based on literature review and expert opinions.

Each product category appears involved in multiple possible cyberattack cases, all of them with an assigned impact and likelihood level. A general risk value is calculated below for each of these product categories to finally present the risk profiles.

Acknowledgement of study limitations

The methodology followed in this study generated a series of risk profiles for ICT product categories by sector. Consequently, risk profiles were calculated at the consolidated level, without looking at specific product’s risk level. Such an approach means that all products within the same category were considered as if they were simultaneously involved in each attack case. For instance, most products are ranked as medium-high or high risk while some specific products can have high or low level of risks. As the final grade is only a mean, these differences are hidden in the final score that tend to gravitate towards the mean for all product categories.

In addition, every feared event has been presented with a single impact level, without taking into account possible sublevels. For example, “human injuries or death” has been presented as a high impact feared event, considering the worst situation within that event, but no sublevels have been considered — such as the gravity of the injury.

In other words, the chosen methodology covers a wide array of sectors and aim at developing generic risk profile per product category. Consequently, these risk profiles are developed at a macro-level and do not provide details about individual products and their intended use. The core focus of this methodology is to provide a global overview as well as general guidelines that feed the study when developing the different policy options. Nevertheless, the same methodology can be applied at a more granular level as illustrated with the two examples detailed below.

To illustrate the added-value brought by this methodology, Table 23 details two applications cases. Firstly, an example of feared event ("human injuries or death) by end-device in Smart Manufacturing. Secondly, the case of the risk of "personal data theft" in Smart Home software. Additional details are provided for each case, looking at different levels of impact for different attack cases. **Providing such a detailed view for each sector and product is out of the scope of this study.** Therefore, this table should be seen as a demonstration of the full potential held by the methodology developed in this study.

Table 23 Examples of extended risk profile analysis – as indication for future research

EXAMPLES OF EXTENDED RISK PROFILE ANALYSIS – AS INDICATION FOR FUTURE RESEARCH

Smart manufacturing: End devices – Human injuries or death

The following "End devices" products in Smart manufacturing were identified in the first part of this paper:

ICT Category (Smart Manufacturing)	Description
End Devices	
Sensors and cameras	Detect, measure events and transmit information.
Safety Instrument Systems	Sensors, solvers and actuators whose objective is the safety in case of violation of current conditions.
Actuators	Devices that can move or control physical mechanisms or systems.
Mobile devices	Portable devices and the application they operate.
Smart robots, Automated guided vehicles	Industrial robots with "smart capabilities" (e.g. machine learning) designed for complex tasks.

For this category of product, the cyberattack cases that can lead to "human injuries or death" are listed below:

Product category	Risk cases				
	Risk origin	Target objective	Path	Attack method	Likelihood
End devices	Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	1/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	1/3

More granular risk profiles can then be developed looking at sub-levels by feared event. These sublevels can then be described and their impact level scored. The report "Key statistics in the Manufacturing sector in Great Britain"[224], identify two sublevels for "human injuries or death": fatal injuries and non-fatal injuries — the later can then be split between accidents that lead work leave or not.

Feared event	Levels of impact		Impact
Human injuries or death	Fatal injuries (death)		3/3
	Non-fatal injuries	Causing absence from work	2/3
		None absence	1/3

[224] Key statistics in the Manufacturing sector in Great Britain, HSE, 2020

The ENISAS's report "Good Practices for Security of Internet of Things in the context of Smart Manufacturing"[225] provides the following examples of attack against end-product along with an evaluation of their impact:

- Attack against sensors and cameras (modification of measured values / states, their reconfiguration, etc.): Medium-high.
- Attack against the Safety Instrumented Systems (SIS): High.
- Attack against actuators or smart robots (suppressing their state, modifying their configuration): Medium-High.
- Manipulation of mobile devices (e.g. operating panels, smartphones): Medium.

This information can then be combined with our previous steps, providing us with the following table:

Product (End devices)	**Risk cases – with a more detailed assessment of impact**						
	Risk origin	**Target objective**	**Impact level**	**Path**	**Attack method**	**Impact**	**Likelihood**
Sensors and cameras	Hacktivists	Human injuriesor death	Non-fatal injuries, causing absence from work	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	Hacktivists	Human injuriesor death	Non-fatal injuries, causing absence from work	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Safety instrument systems	Hacktivists	Human injuriesor death	Fatal injuries (death)	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	1/3
	Hacktivists	Human injuriesor death	Fatal injuries (death)	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3
Actuators	Hacktivists	Human injuriesor death	Non-fatal injuries, causing absence from work	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	Hacktivists	Human injuriesor death	Non-fatal injuries, causing absence from work	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Mobile devices	Hacktivists	Human injuriesor death	Non-fatal injuries and non-absence	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	1/3	1/3
	Hacktivists	Human injuriesor death	Non-fatal injuries and non-absence	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	1/3	1/3
Smart robots, Automated guided vehicles	Hacktivists	Human injuriesor death	Non-fatal injuries, causing absence from work	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3

[225] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, 2018

	Hacktivists	Human injuries or death	Non-fatal injuries, causing absence from work	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Using the same calculation methodology that was applied at the product-category level, risk level can be calculated for each specific product as detailed in the table below:

Product category	Feared event	Product	Risk level
End devices (Smart Manufacturing)	Human injuries or death	Sensor and cameras	Medium-Low
		Safety instruments systems	Medium
		Actuators	Medium-Low
		Mobile devices	Low
		Smart robots, Automated guided vehicles	Medium-Low

Smart home: Software – Personal data theft

"Software" products in Smart home were identified in the first half of the study and are reminded in the table below:

ICT Category	Description
Software	
Program (code)	These programs are written for devices within an IoT ecosystem to achieve specific technological objectives.
Operative system	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run.
Mobile app	These programs run on mobile devices, such as tablets and smartphones.
Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.
Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate.

Cases of cyber-attacks against smart home software potentially leading to "personal data theft" are listed in the table below:

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
Software	Cybercriminals	Personal data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Cybercriminals	Personal data theft	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
	Insider attacker	Personal data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Insider attacker	Personal data theft	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3

As for the case of smart manufacturing, the next step is to develop more granular risk profiles looking at sub-levels by feared event. These sublevels can then be described and their impact level scored. The ENISA's report "Recommendations for a methodology of the assessment of severity of personal data breaches"[226] identified the following level of severity for data breaches in Smart Home.

Severity of data breach	
Low	Individuals either will not be affected or may encounter a few inconveniences, which they will easily overcome (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome with some efforts (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).

Taking this into account, the "personal data theft" feared event's levels can be divided as shown in the table below:

Feared event	Levels of impact	Impact
Personal data theft	Individuals may encounter a few inconveniences, which they will overcome without any problem	1/3
	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	2/3
	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties	3/3

The ENISA's report "Good practices for security of IoT"[227] identifies lacking or insecure credentials as one of the most critical issues in software security. Users with insufficient awareness in cybersecurity can choose weak or easy-to-remember credentials that are easy to hijack. Furthermore, restrictions for the definition of new credentials (such as password length restrictions or character use impositions) can lead an upset user to opt for weak codes to shorten the procedure. In this sense, together with the user's lack of experience in terms of cybersecurity, the design and coding of mobile applications and websites can be linked to this weakness.

"Antivirus" programmes appear as the second most critical product in the software category. Although it is not usually a common source of attack, it is a critical system for other devices and systems. "Firmware" and "operating system" appear as the least critical products in the software category. Although update deficiencies or failures can be sources of attack, it is quite rare to find these types of vulnerabilities.

This new information can be added to the list of cyber-attack cases previously identified and applied for each product in the software category as illustrated below:

[226] Recommendations for a methodology of the assessment of severity of personal data breaches, ENISA, December 2013

[227] Good Practices for Security of IoT - Secure Software Development Lifecycle, ENISA, November 2019

Product (Software)	Risk cases – with a more detailed assessment of impact					
	Risk origin	**Impact level**	**Path**	**Attack method**	**Impact**	**Likelihood**
Program (code)	Cybercriminals	Personal data theft (significant consequences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Cybercriminals	Personal data theft (significant consequences)	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
	Insider attacker	Personal data theft (significant consequences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Insider attacker	Personal data theft (significant consequences)	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
Operative system	Cybercriminals	Personal data theft (few inconveniences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	1/3	2/3
	Cybercriminals	Personal data theft (few inconveniences)	Insecure Data storage	Manipulation, abuse and theft of data	1/3	2/3
	Insider attacker	Personal data theft (few inconveniences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	1/3	2/3
	Insider attacker	Personal data theft (few inconveniences)	Insecure Data storage	Manipulation, abuse and theft of data	1/3	2/3
Mobile app	Cybercriminals	Personal data theft (significant consequences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Cybercriminals	Personal data theft (significant consequences)	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
	Insider attacker	Personal data theft (significant consequences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Insider attacker	Personal data theft (significant consequences)	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
Antivirus	Cybercriminals	Personal data theft (significant inconveniences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Cybercriminals	Personal data theft (significant inconveniences)	Insecure Data storage	Manipulation, abuse and theft of data	2/3	2/3
	Insider attacker	Personal data theft (significant inconveniences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Insider attacker	Personal data theft (significant inconveniences)	Insecure Data storage	Manipulation, abuse and theft of data	2/3	2/3
Firmware	Cybercriminals	Personal data theft (few inconveniences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	1/3	2/3
	Cybercriminals	Personal data theft (few inconveniences)	Insecure Data storage	Manipulation, abuse and theft of data	1/3	2/3

	Insider attacker	Personal data theft (few inconveniences)	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	1/3	2/3
	Insider attacker	Personal data theft (few inconveniences)	Insecure Data storage	Manipulation, abuse and theft of data	1/3	2/3

Using the same calculation methodology that was applied at the product-category level, risk level can be calculated for each specific software as detailed in the table below:

Product category	Feared event	Product	Risk level
Software (Smart Home)	Personal data theft	Program (code)	Medium-High
		Operative system (OS)	Medium-Low
		Mobile apps	Medium-High
		Antivirus	Medium
		Firmware	Medium-Low

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

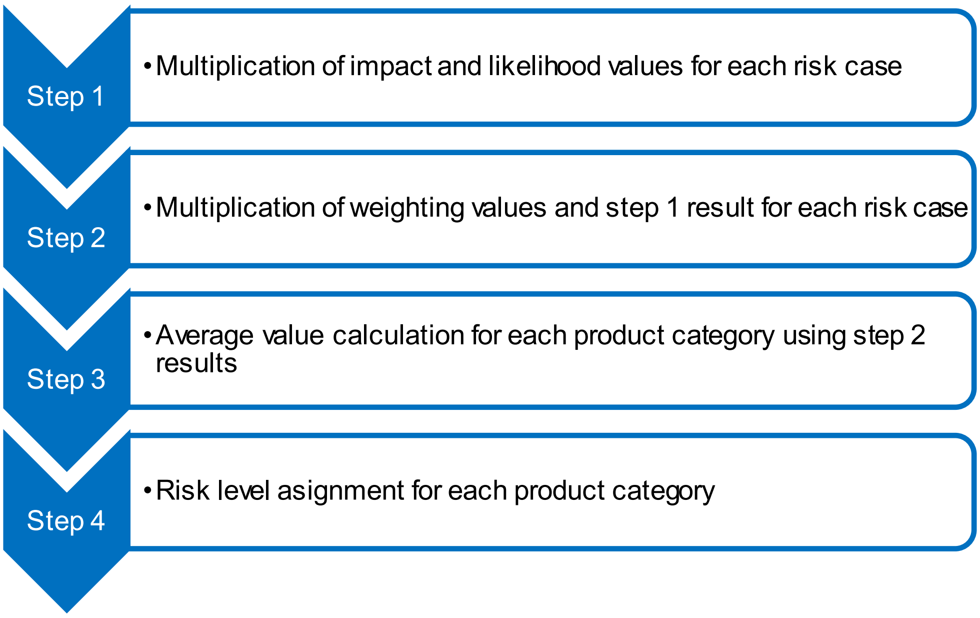
3.2.2.1 Calculation of a general risk value for each product category and sector

As set out in the task objective, generic risk profiles per product category were calculated. Four alternatives were considered to calculate a general risk value for each product category:

1. Using the grade of the product with most elevated risk for the entire category (worst case). It is a simple method, but this way of proceeding gives an exaggerated vision of a category's level of risk. All products are considered as equally risky and the number of cases does not influence the final score. Moreover, as all categories usually have at least one high-risk profile, nearly all categories would be assessed as highly risky.
2. Summing-up the risk values for all cases in each category and classify the categories from highest to lowest. The problem with this method is that the number of risk cases defined for each product category would influence directly on the resulting risk level.
3. Calculating the average value. While this methodology is less sensitive to extreme values, this method's drawback is that it tends to give a medium risk score to all categories. This is because all values have the same weight, with no ponderation given to extreme cases.
4. The fourth and final method that was selected for this study is the weighted average. High risk level cases are weighted higher than those with a low level, as they are considered more important. This method accentuates the difference between cases with low risk and high risk and avoids the drawback from the simple average (method 3). Still, it prevents the final score to be overly influenced by the presence of a high-risk case (as it is the case for method 1).

The steps to calculate the weighted average are detailed in Figure 17 below:

Figure 17 Risk level calculation



Step 1
- Multiplication of impact and likelihood values for each risk case

Step 2
- Multiplication of weighting values and step 1 result for each risk case

Step 3
- Average value calculation for each product category using step 2 results

Step 4
- Risk level assignment for each product category

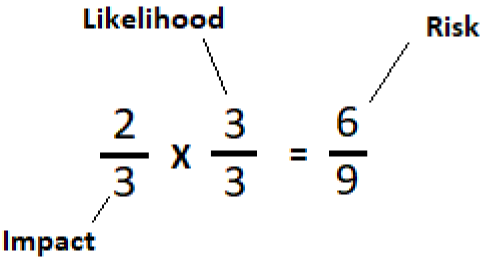
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Step 1: the non-weighted risk value was calculated by multiplying the impact score by the likelihood. This calculation was done for each case. This non-weighed risk level is measured on a 9-level scale.

Taking into account all the possible combinations, five different levels for the risk values are defined (see Figure 18 and Figure 19):

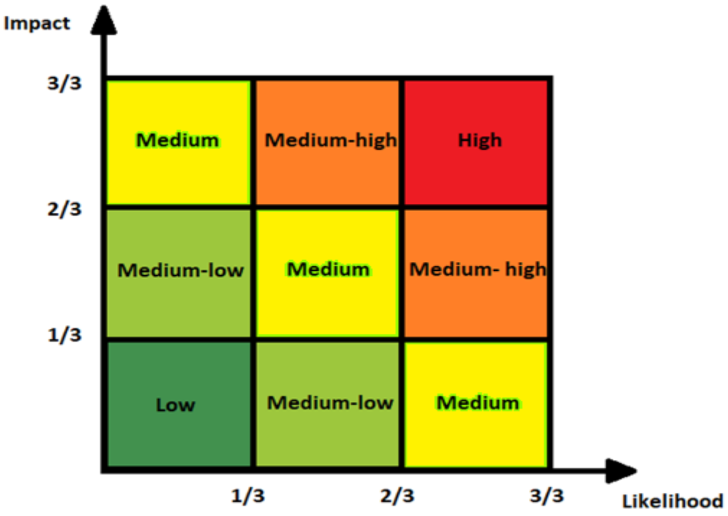
- **High risk cases — 9/9:** high impact and high likelihood.
- **Medium-high risk cases — 6/9:** high impact and medium likelihood cases or medium impact and high likelihood cases.
- **Medium risk cases — 4/9**: medium impact and medium likelihood cases and 3/9 for high impact and low likelihood cases or low impact and high likelihood cases.
- **Medium-low risk cases — 2/9:** medium impact and low likelihood cases or low impact and medium likelihood cases.
- **Low risk cases — 1/9:** low impact and likelihood cases.

Figure 18 Risk level, calculation (example)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Figure 19 Impact-likelihood matrix



Impact			
3/3	Medium	Medium-high	High
2/3	Medium-low	Medium	Medium- high
1/3	Low	Medium-low	Medium
	1/3	2/3	3/3 Likelihood

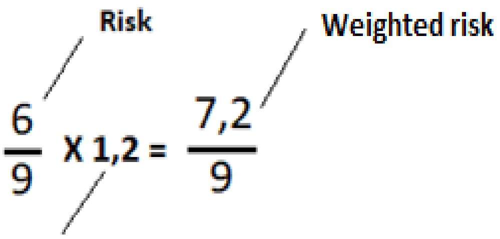
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021). AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW.

Step 2: Different level of risk are assigned different weight. As attack cases with high-risk are more important, they are given a higher weight than cases with a low score.

The weighting factors that are used are the following:

- **High risk cases (9/9)** are weighted with a 1,4 factor.
- **Medium-high risk cases (6/9)** are weighted with a 1,2 factor.
- **Medium risk cases (4/9 or 3/9)** are weighted with a 1 factor.
- **Medium-low risk cases (2/9)** are weighted with a 1 factor.
- **Low risk cases (1/9)** are weighted with a 1 factor.

Figure 20 Weighted risk level, calculation (example)



$$\frac{6}{9} \text{ X } 1,2 = \frac{7,2}{9}$$

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

Step 3: For each product category, the average risk value is calculated using the weighted risk values for each attack case in the category obtained in step 2.

Step 4: Each product category is assigned a score corresponding to its average weighted risk level:

- High risk (weighted average 6.1 to 9);
- Medium-high risk (4.1 to 6);
- Medium risk cases (3.1 to 4);

- Medium-low risk (2.1 to 3);
- Low risk (1-2).

Table 24 below illustrate the calculation procedures (step 1-3) using the example of the software product category for the Energy sector.

Table 24 Weighted risk level calculation example

Product category	Risk cases						Risk value	Weight	Weighted risk value
	Risk origin	Objective	Path	Attack method	Impact	Likelihood			
Software (Code, OS, Apps, Antivirus, Firmware	Cybercriminals	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	3/3	6/9	1,2	7,2/9
	Hacktivists	Communications and network control loss	Commercial hardware and software	Malware, session hijacking	3/3	2/3	6/9	1,2	7,2/9
	Hacktivists	Energy supply disruption	Commercial hardware and software	Malware, session hijacking	3/3	2/3	6/9	1,2	7,2/9
	Insider attacker	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	2/3	4/9	1	4/9
	Hacktivists	Human injuries or death	Commercial hardware and software	Malware, session hijacking	3/3	1/3	3/9	1	3/9
	State-sponsored attackers	Human injuries or death	Commercial hardware and software	Malware, session hijacking	3/3	1/3	3/9	1	3/9
	State-sponsored attackers	Energy supply disruption	Commercial hardware and software	Malware, session hijacking	3/3	1/3	3/9	1	3/9
	State-sponsored attackers	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	1/3	2/9	1	2/9
Average value									4,6/9
Risk level									Medium-high

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and expert opinions.

3.2.2.2 Summary of resulting risk profiles per product category and sector

The same calculation method was applied to reach a risk level per product category and sector. It should be noted that, due to the limitations of the study, the results on the product category level are debatable. For example, the "sector-wide" results should not be taken for granted for all products under one product category. Nevertheless, the indicative results from our simplified assessment, per product category and sector, are presented in Table 25, Table 27, Table 28, Table 29 below, along with some comments.

Additionally, an Impact-Likelihood-matrix is presented per sector (see Figure 21, showing how each product category performs in terms of both risk likelihood (abscissa) and impact (ordinate).

Smart Manufacturing

Table 25 Weighted risk levels for Smart Manufacturing sector

Product category	Risk level (Smart Manufacturing)
End devices	5,4/9
Software	4,2/9
Networks	4,1/9
Security	4,9/9
Programs for decision support	7,5/9
Servers & Systems	3,5/9

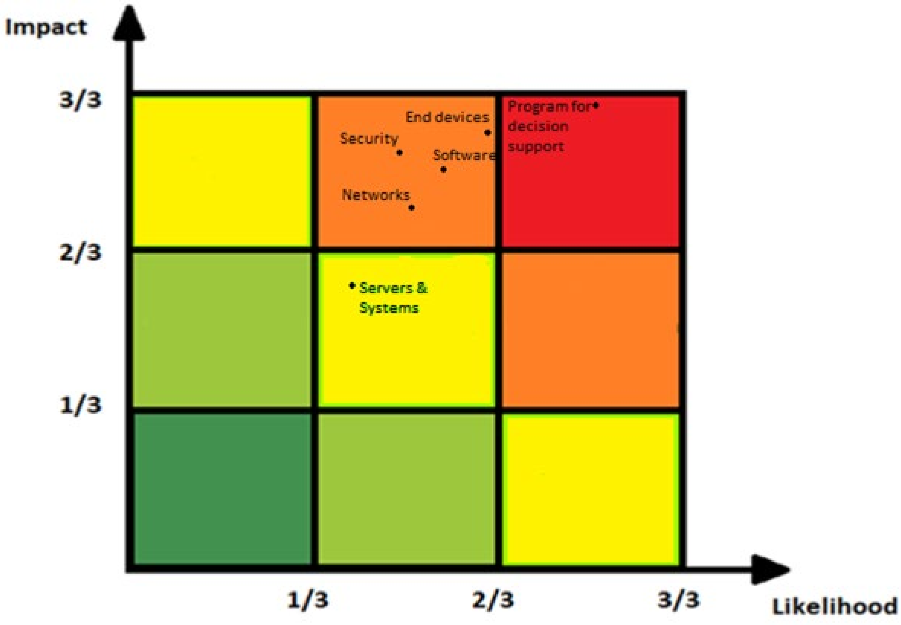
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

The "Program for decision support" product category appears as the highest risk in the Smart manufacturing sector. Almost all other product categories received a “medium-high” risk level.

Sensitive and critical data theft is a feared event with a high-risk value (3/3), and all cases related to this event were considered by stakeholders as the most likely scenarios. In this sense, all the cases in which the programs for decision support category is involved include this feared event, which has made the category level so high.

Contrastingly, scenarios related to Manipulation or loss of control, damage of the batch / product and infrastructure and Human injuries or death feared events were considered as the most unlikely. In addition, the impact of the feared event Manipulation or loss of control, damage of the batch / product and infrastructure is medium (2/3). In this sense, most of the cases in which Servers & systems product category is involved has to do with these feared events, so the final risk level of this category has remained as the lowest level in the sector.

Figure 21 Impact-likelihood matrix – Smart manufacturing



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and expert opinions.

Finance

Table 26 Weighted risk levels for Finance sector

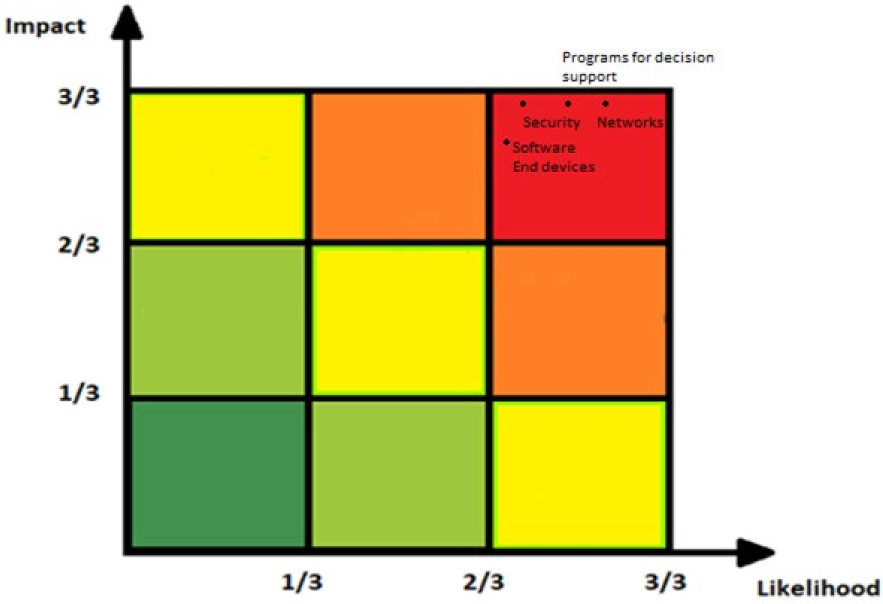
Product category	Risk level (Finance)
End devices	6,8/9
Software	6,8/9
Networks	7,9/9
Security	7,1/9
Programs for decision support	7,2/9
Servers & Systems	

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and expert opinions.

Note: Blank cells mean that information is missing for the combination of sector and product category.

Surveyed stakeholders named two vulnerabilities as the most likely scenarios: "insecure network" and "Lack of user's diligence validating content in emails, messages". Both vulnerabilities typically lead to money theft and theft of confidential information — which are also considered the most impactful events in finance. All product categories are mostly related to scenarios that involve one of these two feared events, which has caused all categories in the sector to present high risk levels.

Figure 22 Impact-likelihood matrix – Finance



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Energy (smart grid)

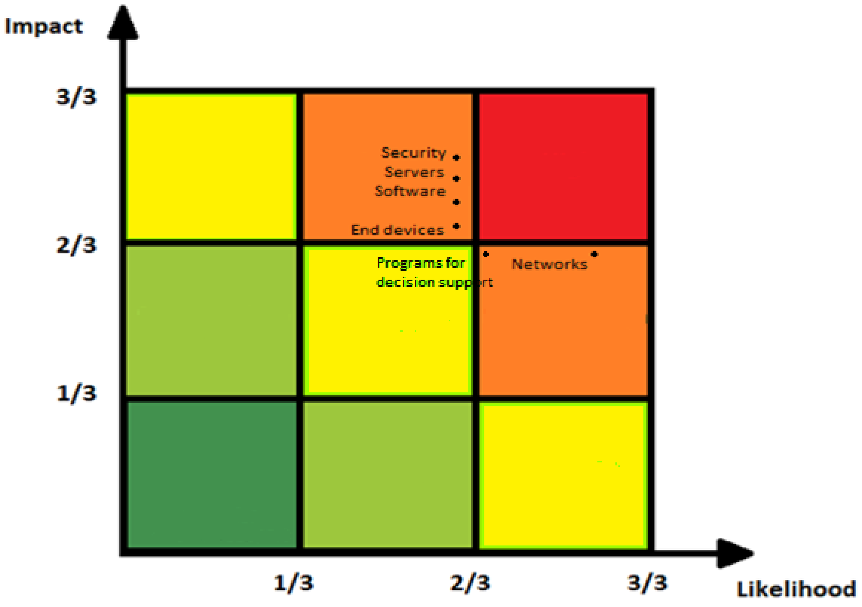
Table 27 Weighted risk levels for Energy (smart grid) sector

Product category	Risk level (Energy)
End devices	4,4/9
Software	4,6/9
Networks	5,1/9
Security	4,8/9
Programs for decision support	4,3/9
Servers & Systems	4,3/9

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

The surveyed stakeholders identified cybercriminals as the most likely attackers and state-sponsored attackers as the least likely. Regarding the feared events, human injuries or death appeared as the least likely one. All energy categories presented risk scenarios of mixed kind (low, medium and high risk), which made the risk profiles rather homogenous without much variation of the results between categories.

Figure 23 Impact-likelihood matrix – Energy (smart grid)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Smart Home

Table 28 Weighted risk levels for Smart home sector

Product category	Risk level (Smart Home)
End devices	6,5/9
Software	7/9
Networks	5,5/9
Security	6/9
Programs for decision support	
Servers & Systems	

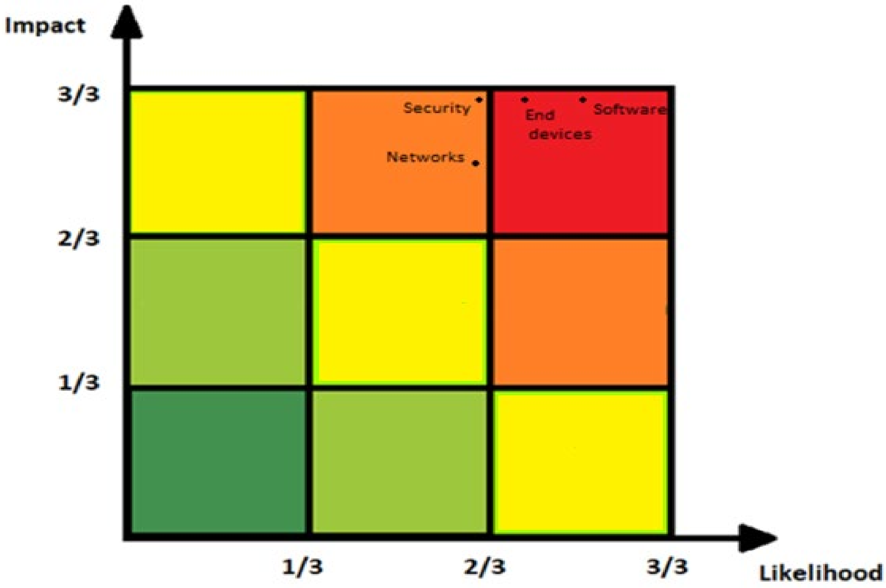
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Note: Blank cells mean that information is missing for the combination of sector and product category.

Stakeholders identified cyber espionage done by cybercriminals, as well as insider attackers, as the most likely attack cases. As cyberespionage is considered a feared event with a high impact (3/3), product categories where such a risk exist achieved the highest level or risk.

Attacks that involve either cybercriminals or insider attackers and cyberespionage as target objectives have been related only to the Software and End devices product categories. Other feared events with the same level of impact such as money theft or personal data theft appear related to Security and Networks product categories, but their level of likelihood is lower.

Figure 24 Impact-likelihood matrix – Smart home



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Transport (ports & airports)

Table 29 Weighted risk levels for Transport (ports & airports) sector

Product category	Risk level (Transport)
End devices	4,3/9
Software	3,9/9
Networks	4,3/9
Security	4,4/9
Programs for decision support	
Servers & Systems	4,4/9

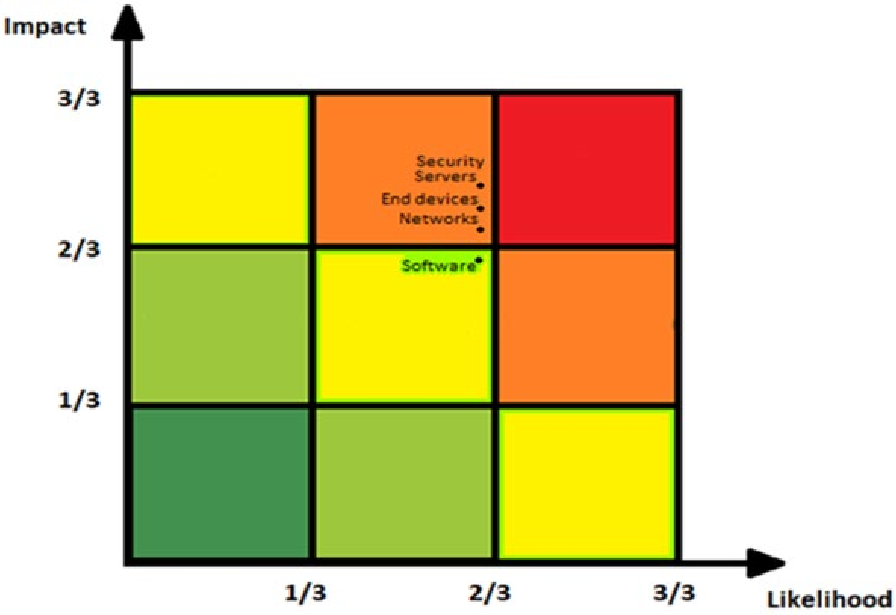
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Note: Blank cells mean that information is missing for the combination of sector and product category.

Stakeholders considered attacks related to the feared event "Sensitive and critical data theft" most likely to occur (3/3); this event has a medium impact level (2/3). "Human injuries or death" and "Shutdown of operations, port/airport paralysis" are feared events with a high impact level (3/3); here the related cases were given a medium level of likelihood (2/3). All product categories are involved in attack cases related to one of these three feared events (Human injuries or death, Shutdown of operations, port/airport paralysis and Sensitive and critical data theft), so the risk level of most categories is medium-high.

Software category has the fewest cases of this type and is also related to several cases with low likelihood level, such as "Cargo and goods stealing" or "Illegal trafficking". This makes the Software category risk level the lowest in the sector.

Figure 25 Impact-likelihood matrix – Transport (ports & airports)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Overall results

Only three types of weighted risk values were observed across the different product categories: medium, medium-high and high. No case scoring either low or medium-low risk have been observed. This result corresponds with what could be expected at the beginning of the study as the large variety of product considered for each category had the effect of making products converge toward higher scores: high or medium-high risk. In addition, high or medium-high risk cases were given a heavier weight. Of course, some categories present more low risk cases than others, but no category exclusively presents low or medium-low risk cases.

Considering these results and aiming to adapt the study results with the terminology of assurance levels used in the EU Cybersecurity Act[228] (basic, substantial and high), the relationship between risk levels, insurance levels and risk profiles was applied (see Table 30).

Table 30 Harmonisation of risk levels, assurance levels and risk profiles

Risk levels per product category in our study	Assurance levels in EU Cybersecurity Act
High risk	High assurance level
Medium-high risk	Substantial assurance level
Medium risk	
Medium-low risk	Basic assurance level

[228] The EU cybersecurity certification framework, European Commission, June 2020

Risk levels per product category in our study	Assurance levels in EU Cybersecurity Act
Low risk	

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

This harmonisation of risk levels into risk profiles is necessary to the formulation of security requirements, assessment methodologies and policy options as defined later in the study. However, this hypothesis should be further validated, beyond the scope of this study, e.g. by stakeholders and/or secondary evidence to ensure it is aligned with the reality of the field.

Additionally, while overall product categories results are only corresponding to high and substantial risk profiles, this does not mean that each product within these categories should be considered as such. To ensure relevant results, case by case analysis on product level would be needed.

The indicative results for the different product categories are summarised Table 31 below, with some comments. Again, the limited level of details applied in the study means that the results need to be interpreted with care.

Table 31 Risk profiles per product category and sector

	Smart Manufacturing	Energy	Finance	Smart Home	Transport
End devices	Substantial	Substantial	High	High	Substantial
Software	Substantial	Substantial	High	High	Substantial
Networks	Substantial	Substantial	High	Substantial	Substantial
Security	Substantial	Substantial	High	Substantial	Substantial
Programs for decision support	High	Substantial	High	NA	NA
Servers & Systems	Substantial	Substantial	NA	NA	Substantial

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND EXPERT OPINIONS.

Note: Cells with "NA" indicates that the information is missing for the combination of sector and product category.

Looking at **product categories**, end devices appear as the most critical, followed by software. According to the "2020 Unit 42 IoT Threat" report, 41% of attacks exploit device vulnerabilities[229].

The human factor is crucial and it should be cautiously considered across all sectors and product categories. Preparation and experience of the end-users are very important factors to take into consideration when assessing how cyber secure a system really is.

[229] The 2020 Unit 42 IoT Threat Report, Palo Alto Networks, March 2020

Finance appears as the **sector** with the highest risk. This can be explained by the fact that, according to the World Economic Forum (WEF), the financial sector account for 21% of all cyber-attacks [230]. The WEF also highlights the manufacturing sector as a likely target, accounting for 13% of all cyber-attacks.

Smart home also has high risk levels, but only in some of its product categories. This is because even though Smart Home is not subject to a lot of attacks —neither in absolute nor relative terms — it is also the sector with the lowest level of preparation.

However, high-risk levels do not have the same impact depending of the sector. Indeed, cyber-attacks against Smart Home systems do not have an impact as critical as an attack that would manage to shut down the entire Energy smart grid.

Limitations

As already mentioned above, the methodology for the risk profiles development holds some important limitations and simplifications, which are linked to time- and budget restrictions of the study. The risk profiles are developed at a macro-level and do not provide details about individual products or their intended use. They provide a global overview and indicative input for developing the different policy options. The assessment of likelihood of the different risk cases are based on desk research combined with expert views from a limited number of focus groups and interviews in the five sectors covered. Furthermore, the experts were only asked their view with respect to one sector. Due to these simplifications the results need to be interpreted with care. For example, the risk profiles presented in Table 31 do not take into account possible differences when comparing between sectors. More detailed assessments would need to be done to be able to have comparable results among sectors (see example of extended analysis in Table 23 above).

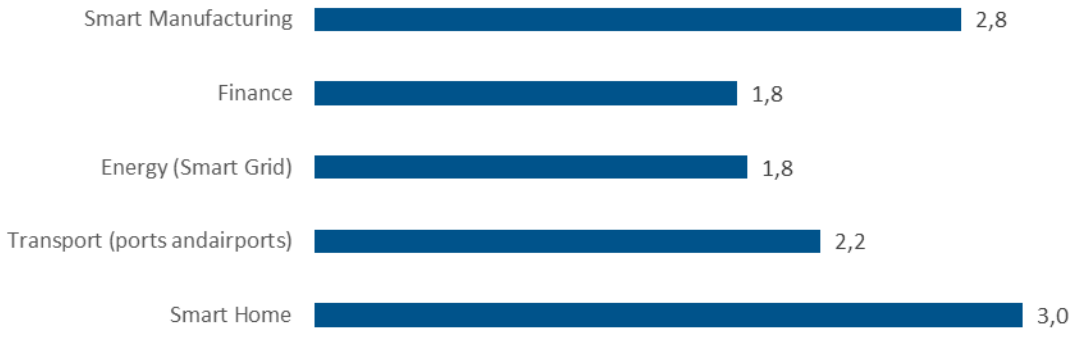
Additional results from the Targeted Consultation

Complementing the single-sector views received from Focus Groups and Interviews, the Targeted Consultation was utilised to try to get a general vision of the relative risks between sectors. Respondents were asked to compare the five sectors covered by the study and rank them in terms of how severe cybersecurity threats they are facing (1-Highest threat; 5-Lowest threat).

As shown in Figure 26below, respondents thought that Finance and Energy (Smart Grid) faced the highest threats, followed by Transport (ports and airports), Smart Manufacturing and Smart Home. There were no significant differences between respondent types.

[230] The Global Risks Report 2020, World Economic Forum, 2020

Figure 26 Comparison of sectors in regards to the severity of cybersecurity threats they are currently facing (1-Highest threat; 5-Lowest threat)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

The study already indicated the Finance sector as one with high level of risk for all product categories (where information was available). This additional result also places it as the one with the highest threat level compared to the rest of the sectors studied.

Regarding the Energy (Smart Grid) sector, the risk levels per product category indicated by the study are not excessively high. However, the results from the targeted consultation show that, together with Finance, it is the sector considered to face the most severe threats.

For the Smart Home sector, the study showed high levels of risk for two product categories. The targeted consultation shows that it is considered to face less severe threats compared to the other sectors. Again, this can be linked to that the potential impact is lower than that of an attack in, for example, the Energy sector.

Conclusions on upcoming work and future research

For the development of policy options within the scope of this study there are some important considerations to bear in mind. The results from the risk profile development indicate that it is not possible to define single risk profiles per ICT product category or per sector. Also, the risk profile of a specific ICT Product may vary between sectors.

As identified during the Second Workshop, taking into account the intended use of the product to better define the risk profile for each ICT Product could be one way of improving the accuracy of the results. Depending on the policy option developed in the study, such extended risk level analysis could be implemented on a case by case basis by the manufacturer. The intended use should serve as a way to identify the most relevant threats (through threat modelling) and overall risks and help to refine the results of the risk assessment.

4 Selection of cybersecurity requirements

The Section proposes a generic lifecycle which can be applied to ICT products as well as the cybersecurity activities which can emerge during the lifecycle. Additionally, the Section identifies a set of Essential Requirements and security requirements which should be applied on ICT products, as well as the assessment activities which enable to evaluate the overall security level of the product against risks.

The generic lifecycle for ICT products proposes a distinction between the different phases an ICT product is expected to go through (before it is placed on the market, while on the market and when it is removed either by the manufacturer or the user). Additionally, the lifecycle also offers a distinction between the software and the hardware path of the product. Finally, a set of cybersecurity activities which can be helpful to the security of the ICT product are evidenced, as well as the key stakeholders which will be present in the product lifecycle. This serves as a basis to help to map requirements and responsibilities during the product lifecycle.

To ensure the security of the product, the study proposes a set of eight Essential Requirements which apply to most products, such as the requirement to “Conceive the product to be secure by default and by design” or to “Protect the data and privacy of the user”. The Essential Requirements aim to be aligned with the NLF mechanisms (such as risk assessments and assessment methodologies), although an additional complexity exists due to the fact that product security must be addressed throughout the lifecycle, and engage more stakeholders than the manufacturers.

Additionally, the study highlights a set of security requirements which contribute to the fulfilment of the Essential Requirements. These security requirements, based on industry standards and best practices, propose a granular approach based on the risk profiles associated to the product category as well as the sector in which the product is placed (such as the financial sector or the industrial sector). Moreover, the security requirements could lead to the presumption of conformity against the associated Essential Requirements, as defined in the NLF.

Finally, assessment activities have been identified to evaluate the conformity of a product against the security requirements. The resulting assessment activities have been identified through an analysis of several certification schemes in place on the market as well as through desk research. The study finally offers a mapping of the assessment activities for each risk profile. It should be noted that although the assessment activities were identified through certification schemes analysis which involves that assessment activities are performed by third parties (because these assessments are in principle applicable to products with higher risk profiles), the same activities may also be carried out by the manufacturers (self-assessment).

4.1 Generic life cycle model for ICT products

4.1.1 Introduction

ICT products can be very different from one another, as they vary greatly in shape, purpose, risk profiles, sectors, technologies involved, etc. Nonetheless, all products must be protected, and requirements must be applied on product to ensure their cybersecurity. These requirements could be specific or common to all and must be integrated to the product throughout its lifecycle.

Therefore, in order to be able to map any cybersecurity requirement for a product and ensure they are taken into consideration throughout the life of a product, the study aims to present a model that will be relevant for most ICT products, while some product-specific phase could be missing.

Through the lifecycle, the following research questions are expected to be answered:

- What are the key stages involved in the life of an ICT product?
- What are the links between each of the key stages defined earlier?

The Lifecycle Model was defined through different steps:

1. Definition of the scope and expected format of the lifecycle.
2. Selection of an existing model close to ICT product.
3. Challenge of the preliminary model through literature review.
4. Feedback from stakeholders during a Focus Group on Cybersecurity Activities.

The model chosen was the one from Wavestone in regard to the lifecycle of Connected Device Internet of Things (IoT) products [231]. This model was constructed based on multiple engagements with various industries, and external input from field experts. The model was chosen as IoT products have a fairly complex lifecycle which can include multiple paths based on user changes or changes of IoT clusters (grouping of IoT devices/sensors interacting with one another), while also offering an appropriate level of abstraction which could be used for all products. It was deemed possible to simplify the model by removing the IoT focus and generalise some stages to all ICT products.

4.1.2 Scope of the lifecycle for an ICT product

In this study, the **product lifecycle is defined** as:

"The stages in a particular product's existence: introduction, growth or increasing sales, maturity (= slow or no increase in sales) and decline or reduction in sales." [232]

In order to frame the study, the following **study scope** is proposed as the basis for the underlying lifecycle model:

"The lifecycle of an ICT product starts with the ideation phase to define what the ICT product will consist of, and finishes when the ICT product has been revoked with all unnecessary data removed from both the product and services related to the product (such as Cloud-based services)."

4.1.3 Proposed lifecycle

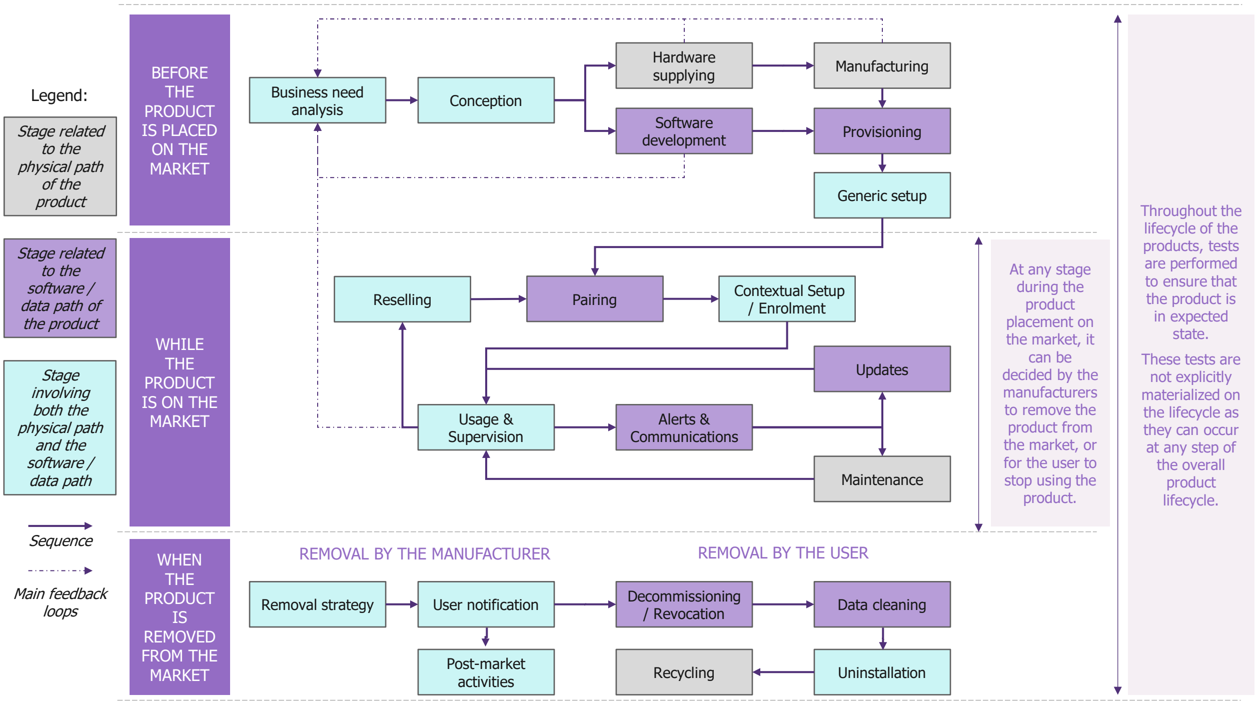
The proposed lifecycle model for ICT model is described in Figure 27:

Readers should keep in mind that this is a generic model, aiming to fit most ICT products. There might be typologies of products for which a stage could be skipped (e.g.: data cleaning for a product not holding any sensible or confidential data) or reversed (e.g.: pairing and contextual setup).

[231] Connected Device Life Cycle: How does it impact the viability of IoT projects?, A. Morize, R. Pointerau, 2020

[232] Information available at : https://dictionary.cambridge.org/dictionary/english/product-life-cycle

Figure 27 Proposed ICT Product Lifecycle


Legend:
Stage related to the physical path of the product
Stage related to the software / data path of the product
Stage involving both the physical path and the software / data path
Sequence
Main feedback loops
BEFORE THE PRODUCT IS PLACED ON THE MARKET
WHILE THE PRODUCT IS ON THE MARKET
WHEN THE PRODUCT IS REMOVED FROM THE MARKET
Business need analysis
Conception
Hardware supplying
Software development
Manufacturing
Provisioning
Generic setup
Reselling
Pairing
Contextual Setup / Enrolment
Updates
Usage & Supervision
Alerts & Communications
Maintenance
REMOVAL BY THE MANUFACTURER
REMOVAL BY THE USER
Removal strategy
User notification
Post-market activities
Decommissioning / Revocation
Data cleaning
Recycling
Uninstallation
At any stage during the product placement on the market, it can be decided by the manufacturers to remove the product from the market, or for the user to stop using the product.
Throughout the lifecycle of the products, tests are performed to ensure that the product is in expected state.
These tests are not explicitly materialized on the lifecycle as they can occur at any step of the overall product lifecycle.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

The different stages are detailed in the tables below. It should be kept in mind that in order to simplify the lifecycle diagram, only some feedback loops to the Business Need Analysis phase have been highlighted. However, depending on the system development methodology or project management methodology chosen, more feedback loops might occur between stages, or even within stages.

Additionally, also for simplification purposes, testing stages have not been displayed. It should however be noted that tests are being conducted at most stages, depending on the product's context, to ensure that the product is in the exact state that is expected at the end of the stage. For example:

- Quality tests
- Feature tests
- Compliance tests
- Security tests
- User acceptance tests
- Etc.

Table 32 Lifecycle stages before the product is placed on the marketTable 32 presents the main stages the product will go through before it is placed on the market.

Table 32 Lifecycle stages before the product is placed on the market

Description	Example of cybersecurity-related activities
BUSINESS NEED ANALYSIS	
The lifecycle starts with the ideation phase to imagine the product. Once this has been produced, a thorough analysis of the business needs for the product is performed. Based on the results of the analysis, the key user features and requirements to consider for the products are defined. The key stakeholders who will intervene during the whole project are identified.	During the analysis, the qualification of the risk level required for the product, the framing of necessary security investment (both financially and human-resource wise) as well as preliminary security stages and guidelines for the projects are provided. This stage is usually the basis on which "Integration of Security into Projects" (or ISP) is built in order to provide the necessary security requirements for the product. It is also the primary stage to enable "security by design"[233].
CONCEPTION	
During the conception phase, the design as well as the architecture of the product is defined. This phase is essential to the process of making the product as it mandates the final outline for both the software and hardware part of the product. The design takes into consideration the specific business needs as well as future features, both functional or not, including the security-related features which could be difficult to implement once the product is on the market due to missing hardware or software engineering issues[234]. The ability to update the product is therefore paramount to overcome these limitations. Prototyping is also an important part of the conception phase, where the specification for physical components will be chosen to ensure the product can be assembled.	Key cybersecurity activities performed during this stage are usually risks assessments and risk analysis and identification of security features and relevant standards to overcome the risks, architecture and network reviews[235], definition of hardening guides and building the requirements for subcontractors involved in the making of the product (such as hosting providers or service providers). An official validation from a Security Officer can be required at the end. During the prototyping phase, the security features must also be included, and the related technical requirements and costs must be evaluated to ensure their application is viable in the final product[236].

[233] ENISA, "Good Practices for Security of IoT - Secure Software Development Lifecycle", 2019

[234] McKinsey, "Shifting gears in cyber security for connected cars", 2017

[235] Andreas Riel, Christian Kreiner, Georg Macher, Richard Messnarz, "Integrated design for tackling safety and security challenges of smart products and digital manufacturing", CIRP Annals, Volume 66, Issue 1, 2017

[236] Lee, Edward. (2008). Cyber Physical Systems: Design Challenges. Electrical Engineering and Computer Sciences.

Description	Example of cybersecurity-related activities
HARDWARE SUPPLYING	
The hardware supplying is a critical stage in order to ensure the physical parts of a product are brought together before it is manufactured. Based on the business needs defined earlier as well as the requirement sent for hardware parts during the conception face, parts of the product will be either manufactured or supplied through procurement and supply chain.	As the hardware supplying is often outsourced, the cybersecurity activities during supplying often relies on contractual engagements from third party suppliers, as well as testing of the provisioned hardware[237].
SOFTWARE DEVELOPMENT	
As ICT product relies on IT technologies, software is another critical piece in the making of an ICT product, which often provides the "intelligence" of the product. The software development has its own lifecycle, often refers to as the Software Development Life Cycle (SDLC), and can be either done by the manufacturer, the service operator or a third-party.	Integrating security into software is also essential[238]. Depending on the methodology used to manage the development (agile or V-cycle), the security activities will differ, relying nonetheless on the integration of security features, penetration testing or code review.239 Additionally, secure development practices and methodologies have to be integrated240. Mechanisms to enable detection (such as logging mechanisms) should be forecasted.
MANUFACTURING	
The manufacturing phase is the phase where the product come together in its final physical form, by receiving and storing components, assembling or transforming the different hardware parts mentioned in the hardware supplying phase and testing the result upon assembling. For some products, parts of software could be integrated during the manufacturing phase.	Security tests can be performed after the manufacturing phase, to ensure the physical product does not expose irrelevant interfaces or displays unnecessary information or through hardware hacking. The global testing process should also include security aspects.

[237] Tony Scott, "Supply chain cybersecurity: A Report on the Current Risks and a Proposal for a Path Forward", 2018

[238] Aakanksha Rastogi, Kendall E. Nygard, Cybersecurity Practices from a Software Engineering Perspective, International Conference on Software Engineering Research and Practice, 2017

[239] Jøsang A., Ødegaard M., Oftedal E. (2015) Cybersecurity Through Secure Software Development. In: Bishop M., Miloslavskaya N., Theocharidou M. (eds) Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham.

[240] Donna Dodson, Murugiah Souppaya, Karen Scarfone, Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), NIST White Paper, 2020

Description	Example of cybersecurity-related activities
PROVISIONING	
Once the physical product is finally brought together, the final software is provisioned on the product to make it complete. The provisioning of software is usually done physically, either by a human operator or through automated channels, but can be done through a network if an existing software/firmware is already present on the product.	To ensure the cybersecurity of the product, tests can be performed on the product to ensure the software installed on the product is safe and secured, as well as integrity checks on the software installed.
GENERIC SETUP	
Once the product has been provisioned with software, an initial setup is performed so that the product is as ready as possible for its usage by the customer. This will allow the product to be in its default configuration.	To ensure the product is safe before it is placed on the market, the product must be provided with a secured and documented configuration by default. A penetration test is recommended as it is the last phase before the product is ready to be sold.
PAIRING	
Once the product has been purchased, there is a need to pair the product with a user[241] or an entity. This is usually done as the first stage before usage, by the creation of an account on the product if user-specific, of an enterprise subscription for a cloud-based product for a company, or even by providing a licence number. Autonomous pairing is sometimes used as well. [242]	Depending on the pairing methodology, additional due-diligence might be required to verify the identity of a user or company. The integrity and confidentiality of data exchanged during this phase, as well as reliable authentication processes, are paramount.

[241] Throughout this study, the term user is used. The user is the person which uses the product on a regular basis, and can be both an individual using the product in a private environnement or an employee using it to perform professional duties. It should not be mistaken with the consumers (the one purchasing the product) or the technician (a third party which can maintain the product).

[242] J. Han et al., "Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing Using Different Sensor Types," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 836-852.

Description	Example of cybersecurity-related activities
CONTEXTUAL SETUP / ENROLMENT	
Once the product has been paired with a user or an entity, a contextual setup might be required to adapt the product to the context and usage in which the product will be used (for example, adding features on a mobile phone). Additionally, if the product is part of a cluster of products (for example in Internet of Things context), the product will need to be enrolled in an online subscription. All of these steps could be performed by a final user or by technical teams in a corporate context.	As for the generic setup, the provider should make the contextual setup as easy as possible for the user and provide the necessary information to help with the secure setup. During the enrolment phase, the provider must ensure that the information is received only from an authorised user and not a third party.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Table 33 presents the main stages when the product when placed on the market and used in its nominal mode.

Table 33 Lifecycle stages while the product is on the market (in nominal mode)

Description	Example of cybersecurity-related activities
USAGE & SUPERVISION	
This is the standard phase of usage, where the customer uses the ICT product in its nominal mode. During the product usage, the state of the product is monitored constantly to ensure that it continues to perform its duties as required. Based on the information provided by the product as well as external sources, the service operator and the manufacture ensure that the product remains safe and secure. Users also notify issues to the service operator to share problems they are phasing with the product or additional features they would like to see.	In some cases, providing best practices to the customer might be required to ensure the product is used in a secure manner and to provide cybersecurity awareness to the user. The surveillance aspect should also include security and could be performed by monitoring of actions from the user or device to ensure it used adequately or collecting data relevant to security. Additionally, the technologies and components used by the product must be monitored to detect any security vulnerability.

Description	Example of cybersecurity-related activities
ALERTS & COMMUNICATIONS	
Based on the surveillance phase, alerts might be sent to the customer/user to notify him of malfunctions or security risks. The alerts can be sent on the device itself or through other channels (email, phone, etc.). Clear communications are important to ensure the user can trust the message received as well as for the user to understand which steps it must take to ensure the product is back to a working state.	An incident management capability is usually required to qualify, investigate and respond to alerts. To ensure notifications are passed on in a secure manner, the channels on which alerts are sent must be secured and known from the customer. Communication processes with the authorities have to be identified to facilitate the work in case of significant incidents.
UPDATES	
In order to keep the product relevant and safe for the user in terms of functionalities, the manufacturer and service operator will prepare updates to be implemented on the software components of the product. These updates can be done automatically or manually and might need to connect to a specific platform or could be available and performed "over the air".	Before releasing an update, it is important to document the impact of the update (or absence thereof) on each version of the product and notify the user accordingly[243]. Risk analysis, product reviews and tests could be performed depending on the product type and the importance of the update. The update mean should also be evaluated[244]. On the product side, the integrity of an update should be verified, as well as the effectiveness of the update once applied.
MAINTENANCE	
As physical components can also break down, the ICT Product maintenance is part of the lifecycle. The maintenance can be performed by the user itself, by the manufacturer or by a third party provider (if preferred by the manufacturer and/or user).	The physical components replaced are integrated to the end-of-life cycle if they could contain data or software. Additionally, the manufacturer or maintainer must ensure that the newly added part is at an equivalent level of cybersecurity[245].

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

[243] Adrian Baranchuk, Bryce Alexander, Debra Campbell, Sohaib Haseeb, Damian Redfearn, Chris Simpson, Ben Glover, "Pacemaker Cybersecurity", Vol 138, Issue 12, Circulation, 2018

[244] Kevin Dunn, "*Automatic update risks: can patching let a hacker in?*", Network Security, Volume 2004, Issue 7, 2004, Pages 5-8, ISSN 1353-4858

[245] I. Ilhan and M. Karaköse, "Cybersecurity Framework for Requirements of Repair, Update, and Renovation in Industry 4.0," *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, Ankara, Turkey, 2019

Table 34 presents the main stages the product will undergo when going through a change of customer or user.

Table 34 Lifecycle stages while the product is on the market (when changing customer/user)

DESCRIPTION	Example of cybersecurity-related activities
RESELLING	
For many products, there will be many customers which will be using the device across this lifecycle. The reselling stage requires the product to be put back on a marketplace and sold/given to a new customer, or a product component can be replaced by another one. The product can also be broken down in different parts and remodelled to be integrated in a different product. Before the object is physically exchanged, the data / authentication related to the previous customer is removed and the enrolment of the product if existing is removed.	For certain products, the ability to wipe user-related data from both the product and associated online systems could be required, as well as from any-cloud based tenants, to perform the de-enrolment of the product.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Table 32 Lifecycle stages before the product is placed on the marketTable 35 presents the main stages the product will go through when removed from the market by the manufacturer.

Table 35 Lifecycle stages when the product is removed from the market by the manufacturer

Description	Example of cybersecurity-related activities
REMOVAL STRATEGY	
Before the product is about to be removed from the market, the manufacturer should define its removal strategy for the product on different aspects: what services will be maintained even after the production/distribution is over, how the communication to consumers will happen, if compensation or replacement by a supported product will be provided, if extended support will be available.	The security of the product post-market should be addressed in the removal strategy, especially when it comes to security patches and vulnerability monitoring and disclosure (either by the provider or by third party groups (such as Information Sharing Agreements) as well as the monitoring of potential breaches on the product.
USER NOTIFICATION	
The user notification is an essential part of the removal of the product, as the user needs to decide on whether it will keep using the product, and if so in which conditions. The manufacturer should provide the users with all the necessary information for them to make an informed decision.	The user notification should be made in such a way that the maximum share of users is made aware of the removal of the product. The information should be provided for the user to make its decision based on the additional risks which will be present after the removal (such risks needs to be highlighted).

Description	Example of cybersecurity-related activities
POST-MARKET ACTIVITIES	
Depending of the removal strategies, additional activities might be still happening after the removal of a product, depending on the typology of the product. In context where the product is expected to remain in use, optional support might be provided, or maintenance through third parties.	Different post-market activities can happen to help to maintain the cybersecurity level of the product: security updates can still be provided for a limited time after the production/distribution period is over, the steering of Information Sharing Agreements group for vulnerability monitoring, etc.

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

Table 36 presents the main stages the product will go through when removed from the market by the user.

Table 36 Lifecycle stages when the product is removed from the market by the user

Description	Example of cybersecurity-related activities
DECOMMISSIONING / REVOCATION	
When the product is reaching its end of life, it is removed from the market. If connected to an online platform, the product is disabled, and sessions are closed. Additionally, the access right of the product are removed and the pairing between the product and the platform is disabled.	Secure decommissioning should be available from the start of the product. Controls must be performed regularly to both detects products which might have reached their end of life (such as unused products) as well as ensuring that decommissioned products have effectively no presence nor access rights. Users and data could also be removed from the database if they are not expected to receive alerts or if data is not expected to be kept for the service.
DATA CLEANING	
Once the product has been removed from the market and revoked, data present on the product is removed, so that it comes back to its initial stage before usage.[246]	Sufficient erasure features must be present on the product to ensure that confidential data (at least) is removed effectively from the product. Protection mechanisms should be available nonetheless to block unwished deletion or recover data if erased before the end of life.

[246] James, M. & Szewczyk, P. (2016). Survey on remnant data research: the artefacts recovered and the implications in a cyber security conscious world. In Valli, C. (Ed.). (2016). *The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia (pp.57-65).*

Description	Example of cybersecurity-related activities
UNINSTALLATION	
Once user data has been erased, the final stage to is to remove the software attached to the product, which might contain Intelligence Property or confidential piece of software.	As the product is unlikely to be accessible online at this stage, it must be ensured that uninstallation capabilities are present locally to uninstall the software and that they are followed.
RECYCLING	
Once the product has been removed from all piece of software and data, it can be recycled by breaking it different subcomponents which will be re-employed based on their typology (electronics, plastic, sensors, etc.) or destroyed, or re-used.	For ICT Product hosting highly critical data, the destruction phase is sometimes used as another layer of security preventing from data leak. In this case, it must be ensured that the defined destruction means are systematically followed and that they are efficient (for instance performing random audits).

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

4.1.4 Stakeholders involved in the lifecycle

A large number of stakeholders are involved in the lifecycle of ICT products. As these products are composed of multiple components, both hardware and software based, a high degree of modularity is usually present, and allow for third party providers as well as materials-providers to be involved. Additionally, once the product is on the market, it is possible for a service provider (sometimes different from the device manufacturer) to delegate certain aspects of the lifecycle to third party companies as well (such as maintenance).

The Table 37 describes the different type of stakeholders which can be involved in the lifecycle of a product.

Table 37 List of Stakeholders involved in the product lifecycle

Type of stakeholders	Description	Example
Research and development teams	Research and development teams are involved in the conception stage, by developing software or hardware solutions that will allow the product to perform at its full potential and to be more competitive on the market.	Research teams: Nimbus research center, CEA, internal teams in private organisations
Product Manufacturer	The product manufacturer is the undertaking in charge of building the physical product, by assembling both hardware and software parts. It can itself rely on subcontractors for items or sub-items that are required for the overall manufacturing process.	Transport: Alstom, Siemens, Bombardier Windmills: Enercon, Vergnet, Xant

Type of stakeholders	Description	Example
Suppliers	The suppliers are essential to the making-process of products, as they provide core-expertise in the lifecycle process or sub-parts of the final product. They can intervene on different aspects of the product: Hardware suppliers Software suppliers Services suppliers (such as hosting) Consulting and intellectual services	Software suppliers: Atos, CapGemini, IBM Hosting: DXC, OVH, AWS, Azure
Distributers / Marketplaces	The distributers are the undertakings which aim to make the product available to the public through marketplaces. Depending on the type of products, this can be done by the manufacturer or service operator, or by a third party.	Online marketplace: Amazon, Rakuten, Allegro Multimedia shops: MediaMarkt, Fnac, Saturn
Service provider	The service provider is the undertaking ultimately in charge of ensuring the ICT product keeps functioning throughout its lifecycle. The service provider usually has authority over the suppliers and subcontractors involved in the product lifecycle.	Connected cars: Mercedes, Renault, Volvo Security equipment: Palo-Alto, Fortinet
Customers and users	Users and customers are the final target of most ICT products. Users could either be the purchaser of a product (in a private context – B2B) or employees of a corporation/organisation that has purchased the product (B2C).	B2B: Doctors, service companies, Industry 4.0, etc. B2C: Smart drivers, smart home systems users phone users, etc.
Maintainers	Maintainers are undertakings which are in charge of keeping the product up and running during its lifecycle. The maintainer can take care of either the software part (over-the-air updates or updates on the device) or either the physical parts.	Helpdesk services: Euroconnect, Flat World Solutions Car maintenance: Bosch Services, Euromaster, Midas
Recyclers	Once the product is out of the market, or once it is not used anymore, the product can be recycled by a third-party to renew the physical part of the product, and possibly integrate it in a new product. Such recycled items could contain data or software if they relate to the ICT functions of the product.	Recyclers: Alba, Galloo, Remondis, Praktik System
Security Researchers / Bug Bounty researchers	Security Researchers and Bug Bounty researchers are individuals that look for vulnerabilities on services in products. They are reporting the vulnerabilities to the provider (for free or for a reward for Bug Bounty participants).	Bug bounty platforms: YesWehack, FOSSA, HackerOne
Authorities (national competent authorities, regulatory bodies, market surveillance authorities)	Authorities are public bodies which are ensuring that market players (manufacturers or service operators) are following the rules set for undertakings within the scope they operate (sometimes specific). They also emit recommendations and notice in regard to the security of products.	National competent authorities: ANSSI, BSI, INCIBE, ENISA, European Commission Market surveillance authorities: Telecommunication Office (Austria), State Agency for Metrological and Technical Surveillance - Directorate General Market Surveillance (Bulgaria), Danish Safety Technology Authority
Standardisation bodies	Standardisation bodies are public or private entities which creates standards of requirements which must be followed to ensure the security or safety of a product.	Standardisation bodies: ISO, IEC, NIST
Accreditation bodies	Accreditation bodies are organisations which are entitled to deliverer an attestation to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.[247]	National Accreditation Body: DAkkS, NAH, CYS-CYSAB

[247] ISO/IEC 17000

Type of stakeholders	Description	Example
Conformity assessment bodies	Conformity assessment bodies are organisations which performs conformity assessments on products (as well as organisations, systems and people) to evaluate and rate their conformity against a conformity assessment scheme.	Conformity assessment bodies: T-Systems International GmbH, Bureau Veritas
Certification bodies	Certification bodies are organisations operating a certification scheme, setting specific requirements rules and procedures for a type of products, allowing them to be evaluated against these requirements[248]. These certification bodies can provide licence to laboratories or third parties which have demonstrated their ability to perform such assessment.	Certification bodies: SERTIT, TUV Rheinland Nederland, ANSSI, CSEC
Laboratories [249]	Laboratories are undertakings entitled by accreditation bodies to evaluate the security of a product against security schemes, and to provide certifications for products which have met the requirements of such standards.	Product laboratories: atsec Germany, Epoche and Espri

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

4.2 Essential cybersecurity requirements

In order to provide an appropriate level of safety and security in products, ICT manufacturers should follow best practices and standards which provide guidance on the implementation of security in products, taking into account the risks faced by the product and its intended use. However, such best practices can be numerous. In order to provide a more general guidance which could apply to all products, the study provides a list of Essential Requirements (as defined in section 4.2.1) which can be applied to most ICT products in scope. The Essential Requirements can afterwards be supported by security requirements, which provide a more granular, concrete level of security measures which should be undertaken.

In order to define the Essential Requirements and associated security requirements, the following methodology was followed:

1. An initial desk research was conducted to identify the main standards, academic papers, industry practices and relevant documentations. This initial list was challenged in a Focus Group on Standards, which also served to discuss the current state of usage of standards and best practices in the industry.
2. A first set of security requirements for all product was selected and challenged in a Focus Group on Requirements together with additional questions in regards to the requirements that ICT products should follow during their lifecycle.
3. Another Focus Group on Cybersecurity Activities was conducted to challenge the documentation, the lifecycle proposal and the security activities identified in the ICT product lifecycle. This Focus Group also allowed to connect the security requirements to the product lifecycle stages.

[248] ISO/IEC 17065

[249] Overview of ICT certification laboratories, ENISA, 2018

4. Additional security requirements were identified through the desk research and analysing the final ICT Product lifecycle. The requirements were mapped against 15 standards, best practices and academic papers (both generic and sector specific) listed in Table 38.
5. The proposed list of Essential Requirements for ICT products cybersecurity is deduced from the final list of security requirements.

4.2.1 Essential requirements

Essential Requirements are high-level requirements which are to be applied to a product (and to the services associated with a product, if any). They are not technology-specific and are aligned with the definition provided in the Blue Guide of the European Union[250]:

1. *A large part of Union harmonisation legislation limits legislative harmonisation to a number of essential requirements that are of public interest.*
2. *Essential requirements define the results to be attained, or the hazards to be dealt with, but do not specify the technical solutions for doing so*

The participants of the Second Workshop also mentioned that the Essential Requirements should be aligned with the definition and associated mechanisms provided by the NLF and Regulation (EC) 765/2008, as well as with the conformity assessment mechanisms proposed by the NLF.

The Essential Requirements are supported by the security requirements. These are more granular conditions which allow fulfilling the associated Essential Requirements. Such security requirements could be equivalent to the ones found in standards. The Essential Requirements can be considered as an abstraction of the security requirements which can apply to most products. The identified Cybersecurity Essential Requirements are detailed below in Table 38 Cybersecurity Essential Requirements

Table 38 Cybersecurity Essential Requirements

#	Essential requirements	Description
ES1	**Conceive the product to be secure by default and by design**	The requirement mandates the manufacturer to design and build the product securely so that it can be used in a secure manner from the moment it is purchased.
ES2	**Limit the risks of product compromising**	The requirement mandates the need to include in the product features and mechanisms which protect the product from attackers and threats, and limit their ability to compromise the product.
ES3	**Set up robust identity and access management**	The requirement mandates the need to ensure that the identity of the user and its associated access rights are protected on the product and on the services the product could use.
ES4	**Protect data and user's privacy**[241]	The requirement mandates the need to protect the data provided to the device, as well as to ensure a high level of privacy to users, as requested by the relevant legislation.
ES5	**Raise awareness to ensure a secure usage of the product in its context**	The requirement mandates the need to support the user in its secure usage of the product, and to ease the configuration of the product throughout its lifecycle.
ES6	**Ensure the resilience of the product and associated services**	The requirement mandates the need to provide the best level of availability of the services when it could be affected by incidents, and to limit the possible impacts.

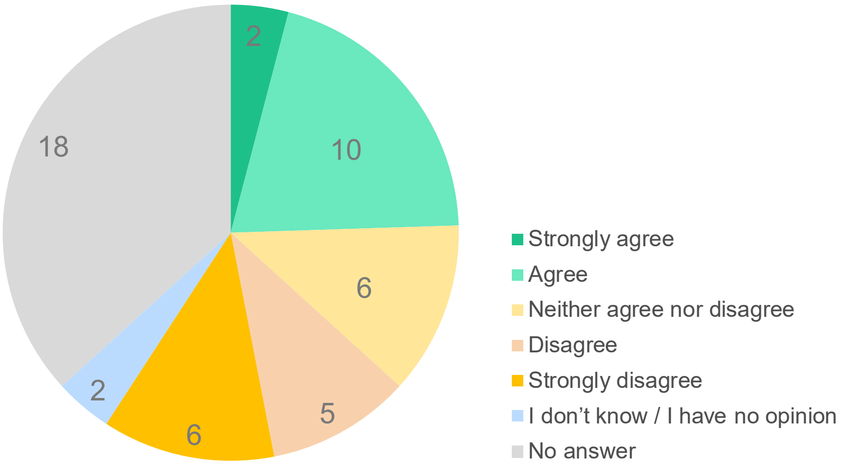
[250] The 'Blue Guide' on the implementation of EU products rules, European Commission, 2016

ES7	**Detect security events and react to security incidents**	The requirement mandates the need to identify threats weighting on the product and to respond to potential attacks through defense mechanisms.
ES8	**Continuously evaluate and improve the security of the product**	The requirement mandates the need for the manufacturer to evaluate the security of the product throughout its lifecycle and to act upon risks and vulnerabilities identified.

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

When presented with the list of eight Essential Requirements (with a different phrasing for ES2[251] and slight wording changes for ES3, ES4, ES5 and ES7[252]), the participants from the Second Workshop offered a mixed answer to the question "Based on your experience, do you agree with the list of Essential Requirements identified for ICT Products?" (see Figure 28). Out of the 31 people which answered the questions, 12 participants agreed or strongly agreed, 11 disagreed or strongly disagreed, six neither agreed nor disagreed and two did not know or did not have an opinion. Additionally, 18 people did not participate to the poll.

Figure 28 Approval of the Essential requirements by the Second Workshop participants



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Second Workshop, N=49

As the Essential Requirements are high-level requirements for ICT products and are not technology specific, they are expected to be found in most products. However, some requirements could be considered not applicable for certain products, based on a Risk Assessment conducted by the manufacturer. This logic is the one used in the Blue Guide, as presented in Figure 29.

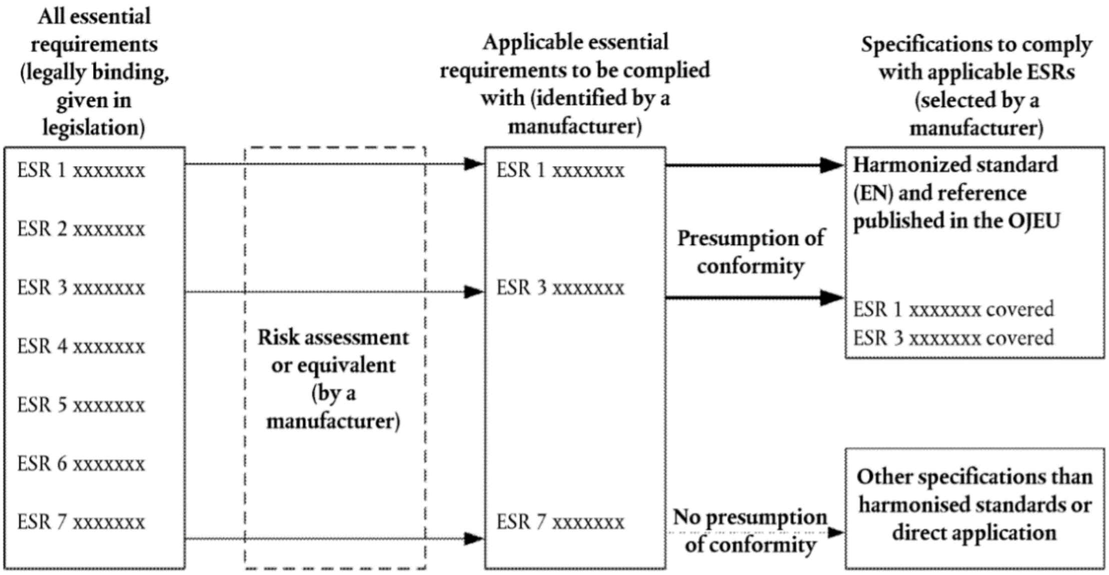
[251] The ES2 presented during the WS was titled "Reduce compromising threats through cyber hygiene", and the term cyber hygiene was questioned as not common enough in the community to be used.

[252] The Essential Requirements were adapted to ensure that they do not seem to address only consumer goods, but to the all ICT products, as it was mentioned during the workshop. The following changes were performed

- ES3: From "Protect the identity and access of the user and product services" to "Protect the identity and access of the user and product services"
- ES4: From "Protect the data and privacy of the user" to "Protect data and user's privacy "
- ES5: From: "Raise the user's awareness to ensure a secure usage in his context" to "Raise awareness to ensure a secure usage of the product in its context"
- ES7: From "Detect and react to security incidents" to "Detect security events and react to security incidents"

The Essential Requirements as defined in the NLF are addressing the manufacturers only, while other obligations will involve the distributors and importers. However, in the case of ICT Products, this division does not allow to address some Essential Requirements which involve the entire lifecycle, such as the market phase and the post market phase. Therefore, the Essential Requirements can also address a broader panel of stakeholders to fully ensure the security of the product throughout its lifecycle.

Figure 29 Interaction between Essential Requirements and specifications


All essential requirements (legally binding, given in legislation)
ESR 1 xxxxxxx
ESR 2 xxxxxxx
ESR 3 xxxxxxx
ESR 4 xxxxxxx
ESR 5 xxxxxxx
ESR 6 xxxxxxx
ESR 7 xxxxxxx
Risk assessment or equivalent (by a manufacturer)
Applicable essential requirements to be complied with (identified by a manufacturer)
ESR 1 xxxxxxx
ESR 3 xxxxxxx
ESR 7 xxxxxxx
Presumption of conformity
No presumption of conformity
Specifications to comply with applicable ESRs (selected by a manufacturer)
Harmonized standard (EN) and reference published in the OJEU
ESR 1 xxxxxxx covered
ESR 3 xxxxxxx covered
Other specifications than harmonised standards or direct application

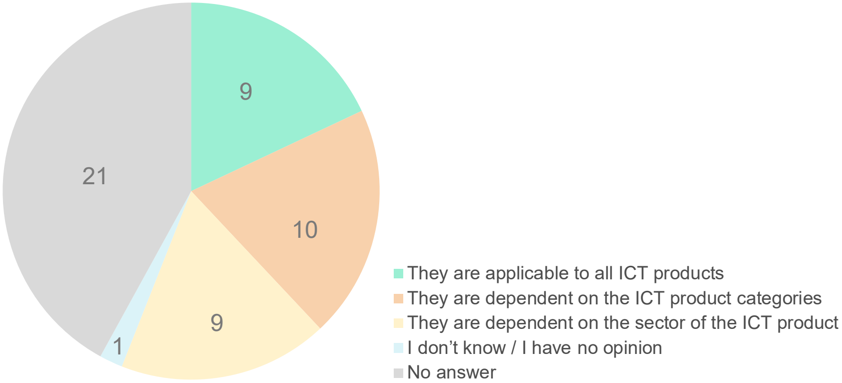
SOURCE: THE 'BLUE GUIDE' ON THE IMPLEMENTATION OF EU PRODUCTS RULES, EUROPEAN COMMISSION (2016)

On the one hand, some participants of the Second Workshop noted that the "intended use" of the product should also be considered during the risk assessment to evaluate the adequation of an Essential Requirement, as it enables to place the product in the context it will be used. On the other hand, other stakeholders of the Focus Groups and the second Workshop have pointed out that the intended use cannot be the only aspect to influence on the risk assessment, as it is difficult for the manufacturer to envision all the contexts in which the product will be placed, as well as the possible "misuse" or "abuse" of the products by customers or malicious actors. Finally, during the Focus Group on Requirements, stakeholders mentioned that Essential Requirements should be considered mandatory for all products if they are named "Essential Requirements" based on the meaning of the word "Essential".

One stakeholder mentioned during an interview that Risk Assessment should be considered with nuance, as it remains possible to orientate the results of a Risk Assessment by choosing hypothesis and scenarios. Therefore, conformity assessments should not rely solely on the result of a Risk assessment, and instead use it as a refining tool.

When asked about the applicability of the Essential requirements, the participants provided a balanced answer (see Figure 30). Out of the 29 people who answered, nine believed that the Essential Requirements apply to all ICT products, 10 that Essential Requirements are dependent of the ICT product category and nine that they are dependent on the sector of the ICT product, while one did not have an opinion or did not know. 21 people did not answer the poll. Some participants mentioned that the intended use of the product should be the factor which influences the applicability of the Essential Requirements.

Figure 30 Applicability of Essential Requirements according to the participants of the second Workshop



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), SECOND WORKSHOP, N=49

Additionally, and as noted by a participant during the Focus Group on Requirements, certain companies and products might need to go beyond these Essential Requirements, depending on the context the products are used in.

Some participants of the Second Workshop pointed out Essential Requirements should be formulated in a way that allows to verify that they are met and fulfilled taking into account the intended use. However, the way some of the Essential are formulated currently do not offer such ability to be verified and/or proven. Instead, the security requirements are expected to provide the level of granularity allowing such verification. In a similar fashion to the NLF, if all security requirements for an Essential Requirement are fulfilled, a presumption of compliance could exist for the product.

Additionally, a discussion occurred on whether the essential requirements should always be attained through state-of-the-art solutions, or if a baseline of simpler security requirements could be acceptable for products with less risk profiles such as very basic ICT products, in case they would face very low risks. The definition of the state of the art level could be defined in additional standards further than the security requirements. An example of such articulation between Essential Requirements, security requirement and state-of-the art proposal could be the following: in order to Protect the identity and access of the user and product services (ES3), secure passwords must be set for users, service accounts for the ICT product and related services (SR). The definition of a secure password (in terms of number and variety of characters, of history of passwords not reusable, etc.) would be defined in an additional document (harmonised standard, industry standard, appendix, etc.).

Finally, the study evaluated how the Essential Requirement would correspond with the security objectives set in the Article 51 of the Cybersecurity Act (see Table 39)

Table 39 Mapping between Essential Requirements and security objectives of Art. 51 of Cybersecurity Act

Essential requirement	a)	b)	c)	d)	e)	f)	g	h)	i)	j)
Conceive the product to be secure by default and by design							✓		✓	
Limit the risks of product compromising				✓			✓		✓	
Set up robust identity and access management	✓	✓	✓							
Protect data and user's privacy	✓	✓	✓							
Raise awareness to ensure a secure usage of the product in its context	*No mapping identified*									
Ensure the resilience of the product and associated services								✓		
Detect security events and react to security incidents					✓	✓				
Continuously evaluate and improve the security of the product				✓			✓			✓

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review

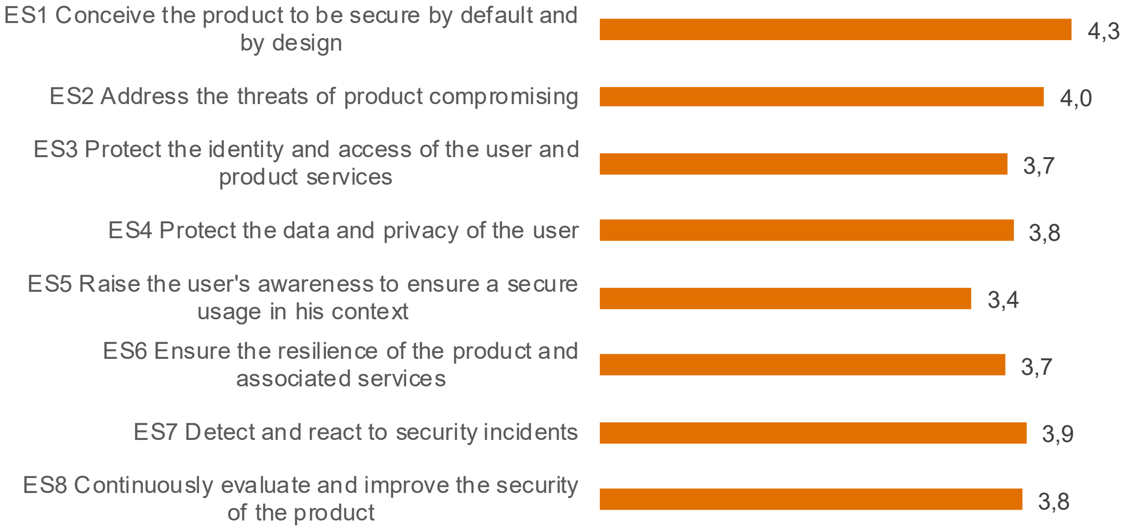
Additionally, although the Essential Requirement (*Raise the user's awareness to ensure a secure usage in his context*) does not appear among the aforementioned security objectives, Article 55(1)(a) of the Cybersecurity Act requires manufacturers of ICT products to provide "guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services".

Additional Results from the Targeted Consultation

When asked in which phases of an ICT product's lifecycle essential requirements should generally apply, the majority of the respondents (76%) thought that Essential Requirements should target ICT products before and after market placement while 22% indicated they should only apply before market placement.

Additionally, consulted stakeholders agreed that the proposed Essential Requirements address the main cybersecurity risks faced by ICT products (1 meaning the Essential Requirement ddoes not address the main cybersecurity risks; 5 that it addresses completely the main cybersecurity risks). The complete details are available in Figure 31. More details and comments are available in Annex V – Target Consultation Results.

Figure 31 Relevance of Essential Requirements against cybersecurity risks for ICT Products



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

4.2.2 Security requirements

The Essential Requirements are supported by security requirements, which are more granular measures which can help to fulfil the associated Essential Requirements (as an example: the security requirement to "*Protect and encrypt traffic using secured protocols"* helps to fulfil the Essential Requirement to "*Protect the data and privacy of the user*"). Such security requirements could be equivalent to the ones found in specifications such as best practices or industry standards. The security requirements can be either technical or organisational measures.

To identify the security requirements, desk research was conducted on a broad set of documentation (academic papers, best practices from National and European authorities, company publications, international standards). Out of all the documents reviewed, the requirements identified were mapped against 15 key documents addressing a broad range of sectors (Internet of Things, Industrial sector, Transportation, Finance). The documentation used for the mapping of security requirements is listed in Table 40. Moreover, the study included a Focus Group on Requirements which validated an initial set of security requirements for all products and helped to get a more comprehensive understanding of the current application of security requirements on the field, as well as the difficulties faced by organisations when integrating security into the product lifecycle.

It should be noted that security requirements are mapped against one Essential Requirement they are primarily contributing to, but they can contribute to the fulfilment of other Essential Requirements. The complete mapping of the contribution of each security requirement to the Essential Requirements is available in the study materials as well in the last column in the sections 4.2.2.1 to 4.2.2.8.

Table 40 Documentation used for the mapping of security requirements

Documentation name	Author	Documentation type	Year	Sector
Essential requirements for securing IoT consumer devices	Meulenhoff & co.	Academic Paper	2020	All
IoT Security Compliance Framework, Release 2.1	IoT Security Foundation	Standard	2020	All
Cybersecurity of medical devices integrating software during their life cycle	ANSM	Best practices	2019	Health
Code of Practice for Consumer IoT Security	UK Department for Digital, Culture, Media & Sport	Best Practices	2018	Consumer goods
Good Practices for Security of Internet of Things in the context of Smart Manufacturing	ENISA	Best Practices	2018	Industry
Good practices for security of Smart Cars	ENISA	Best practices	2019	Automobile
IEC 62443 3-3 and 4-2	ISA	Standard	2020	Industry
IoT Security Top 20 Requirements, UL	UL	Best practices	2020	All
Application Security Verification Standard	OWASP	Standard	2020	All
Baseline Security Recommendations for IoT	ENISA	Best practices	2017	All
FSSCC Automated Cybersecurity Assessment Tool	FFIEC	Standard	2015	Finance
Cyber Security for Consumer Internet of Things, Version 2.1.2 (ETSI TS 303 645)	ETSI	Standard	2020	Consumer Goods
GSMA IoT Security Assessment Checklist (Endpoint)	GSMA	Standard	2018	All
GSMA IoT Security Assessment Checklist (Services)	GSMA	Standard	2018	All
Cyber Security and Resilience of Intelligent Public Transport - Good practices and recommendations	ENISA	Best Practices	2016	Transport

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Additionally, a stratified approach was taken for the security requirements. Three risk profiles were identified for the mapping, as it is commonly used in the Industry. The wording was chosen in alignment with the Cybersecurity Act assurance levels (Basic, Substantial and High) for the sake of consistency. However, the definition of the three risk Profiles is not the one from the Cybersecurity Act, and this choice of terminology should not mean that all products should be certified according to the Cybersecurity Act mechanisms. Additionally, the connection between risk levels and risk profiles can be found in 0.[253]

The security requirements were mapped against different criteria so as to answer the following questions:

1. Which risk profiles should apply the security requirement?
2. What sectors should take into account the security requirement?
3. Is the security requirement addressing the device or the backend service?
4. Which standards provision the need for the security requirement?
5. Which security objectives of the Article 51 of the Cybersecurity Act are addressed through the security requirement?
6. At which stage of the ICT product lifecycle should the security requirement be considered?

[253] If the connection between risk levels and risk profiles evolves, the repartition of security requirements between risk profiles should be reviewed as well to align with the security level.

7. What conformity assessment activities are enabling the evaluation of the security requirement?

Once the mapping was completed, the security requirements were attached to the corresponding Essential Requirements. An example for the mapping is provided in Box 3.

Box 3 Example of security requirement "*Limit the ability to use removal media to the minimum.*"

The security requirement "Limit the ability to use removal media to the minimum." is mainly connected to the Essential Requirement "Address threats of product compromising" (due to the risk of malware on an untrusted removal media), but it can also contribute to the Essential Requirement "Limit the ability to use removal media to the minimum" as it provides a physical network interface to transfer data outside of the device.

This security requirement should be implemented at the device level and aims the products with a substantial risk profile or above. It is particularly relevant for the industrial and financial sector. It was however found only in the FSSCC Automated Cybersecurity Assessment Tool[254].

This security requirement should be considered at the conception, hardware supplying and manufacturing phase. It can be assessed through a design review (possibly a low-level design review).

One important aspect raised by stakeholders during the Focus Group on Standards is that standards should give a clear signal on whether a requirement is mandatory or can be adapted (without having multiple variables to take into account to make such decision), as it makes it difficult to prove the compliance of the product. The participants of this Focus Group also expressed the need for new standards, simpler, easier to understand and allowing adaptable targets (so that they can still be relevant in a constantly evolving threat environment), as the current standards were difficult to be used outside of big organisations. The participants also mentioned that a stratified standards approach would be useful – a low level standard to be applied for everyone, and extra standards depending on the context.

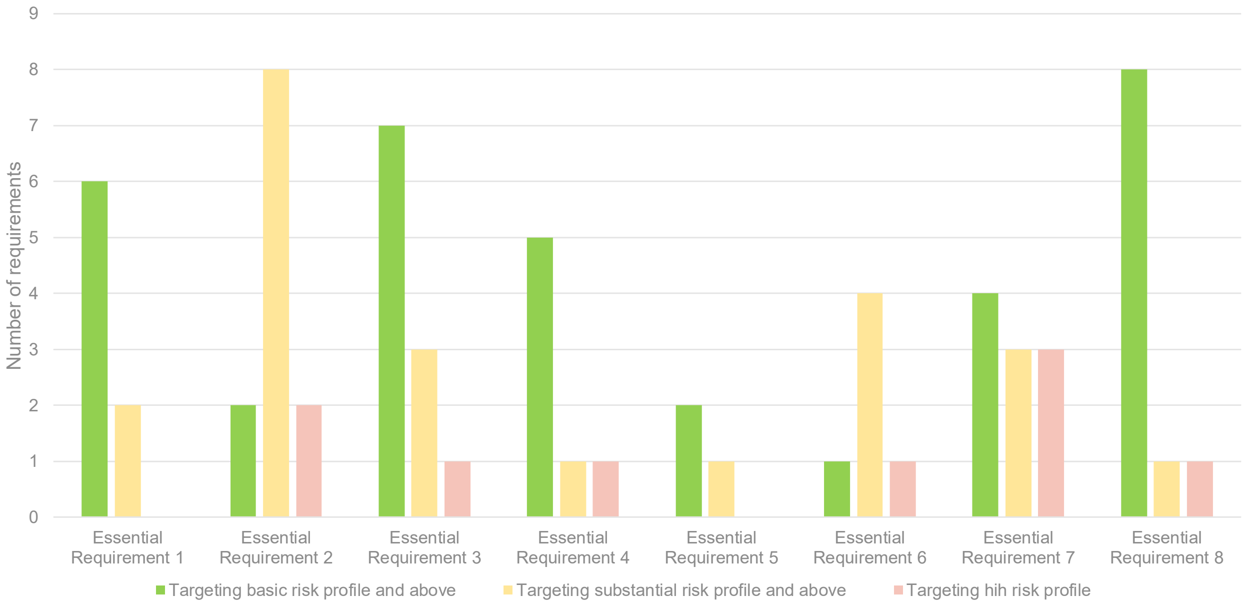
These needs have been considered in the proposed approach for the study. The security requirements are built on a baseline for basic risk profiles which should address all products, and two extra layers of requirements for substantial and high risk profiles. Additionally, there is a possibility to adapt to the context of the stakeholder if a Risk Analysis mandates that an Essential Requirement does not apply in the context of a given product as mentioned above. In such a case, the non-relevance of each underlying security requirements should be justified by the manufacturer, as they might contribute to other Essential Requirements.

The sections below (from 4.2.2.1 to 4.2.2.8) present the security requirements related to each Essential Requirements. Overall, 68 security requirements are identified, with 35 security requirements targeting the basic risk profile and above, 24 substantial risk profile and above and nine targeting the high risk profile.

Figure 32 below shows the distribution of security requirements by Essential Requirements and target risk profile.

[254] Information available at : https://www.ffiec.gov/cyberassessmenttool.htm

Figure 32 Distribution of security requirements by Essential requirements and targeted risk profile



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW.

4.2.2.1 Security requirements primarily associated with Essential Requirement 1

Table 41 bellow shows the security Requirements primarily associated with Essential Requirement 1– Conceive the product to be secure by default and by design.

Table 41 Security requirements primarily associated with Essential Requirement 1

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards [255]	Other ERs addressed [256]
Expose only ports and services strictly needed for the functioning of the product.	Basic and above	All	Both	11	ER2
Systematically conduct a risk assessment based on state of the art methodology and the product intended use to determine cybersecurity risks measures and always base security decisions based on its results.	Basic and above	All	Both	8	ER2
Secure the initial configuration state of the product.	Basic and above	All	Device	7	
Include the necessary reviews and tests to enhance the security during software development and detect potential issues with software security.	Basic and above	All	Both	5	ER8
Limit exposure of unnecessary data or information to limit an attacker's ability to gather information on the targeted product/user.	Basic and above	All	Both	4	ER4

[255] Number of standards addressing the requirement.

[256] Other Essential Requirements addressed.

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards [255]	Other ERs addressed [256]
Follow the least functionality principle when designing the product.	Basic and above	All	Both	1	
Conduct threat modelling to identify attack scenarios and base the risk assessment on the result of the threat modelling.	Substantial and above	All	Both	4	ER2
Design the software to be secure.	Substantial and above	All	Service	1	

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

The need for security to be integrated from the creation of the object was reinforced by stakeholders during the Focus Groups on Cybersecurity Activities. Just like privacy by design and by default has become more and more popular since the adoption of the GDPR, it is necessary to conceive the product to be secure by default and by design. ENISA has proposed several standards and best practices in that direction, such as its releases 'Good Practices for Security of IoT'[257]. The importance of risk assessments, threats modelling and secure Software Development Life Cycle (secure SDLC)[258] has been notably pointed out by the stakeholders.

4.2.2.2 Security requirements primarily associated with Essential requirement 2

Table 42 bellow shows the security requirements primarily associated with Essential requirement 2 – Limit the risks of product compromising.

Table 42 Security requirements primarily associated with Essential requirement 2

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Ensure that service/software/hardware providers contribution to product components ensures an appropriate level of security.	Basic and above	All	Both	6	ES8
Segment the product from untrusted networks.	Basic and above	Industrial, Finance, Transport	Both	2	
Implement self-test mechanisms to verify the security of the product when the product is powered/booted, such as Secure Boot.	Substantial and above	All	Device	10	ES7
Prevent execution of non-validated, external commands, scripts and code present on the system.	Substantial and above	All	Both	9	ES4
Protect the device's critical components (chip, processor, Trusted Platform Modules, critical network elements) against easy physical access and detect alteration of such components.	Substantial and above	All	Device	6	
Integrate a root of trust as Trusted Secure Foundation for cryptographic elements and operations.	Substantial and above	All	Both	5	

[257] "How to implement security by design for IoT", Press Release, ENISA, 2019

[258] Secure Development Lifecycle, E. Keary & J. Manico, OWASP

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Separate user functionalities from management functionalities in the software architecture and implementation.	Substantial and above	All	Both	2	
Transfer updates through encrypted channels.	Substantial and above	All	Device	2	ES8
Limit the ability to use removal media to the minimum.	Substantial and above	Industrial, Finance	Device	1	ES4
Provide mechanisms for dual approval and complex approval chains for critical actions.	Substantial and above	Industrial	Both	0	ES3
Verify the compliance level of other products/devices attempting to connect.	High	Industrial, Finance	Both	3	ES7, ES8
Isolate security functions from non-security functions in the hardware.	High	All	Both	2	

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

As attacks and threats are constantly growing[259], ICT products must more than ever be built to face the compromise attempts which will occur throughout their lifecycle. In order to do so, the product must rely on security functions which will enable an appropriate segmentation against external threats, both in networks and software, and mechanisms to ensure the appropriate level of trust in the ecosystem to which the product belongs. Additionally, relying on trusted providers for hardware, software and services is key, as indirect attacks could represent up to 40% of security breaches [260].

4.2.2.3 Security requirements primarily associated with Essential requirement 3

Table 43 bellow shows the security requirements primarily associated with Essential requirement 3 – Set up robust identity and access management.

Table 43 Security requirements primarily associated with Essential requirement 3

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Require authentication before giving access to network interfaces.	Basic and above	All	Both	14	ES2
Do not store credentials insecurely on services or devices.	Basic and above	All	Both	11	ES4
Design and implement fine-grained authorisation and access rights management mechanisms on the product and on the product-related platforms if existing.	Basic and above	All	Both	11	
Set secure passwords for users, service accounts for the ICT product and related services.	Basic and above	All	Both	10	ES2
Force system defaults values (passwords, certificates or keys) to be modified prior to initial operations.	Basic and above	All	Device	10	

[259] Cost of cyber crime study 2017 - insights on the security investments that make a difference, Accenture, 2017

[260] Innovate for cyber resilience - Lessons from leaders to master cybersecurity execution, Accenture, 2020

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Require machine-to-machine and subcomponent authentication, with appropriate roles set for service accounts.	Basic and above	All	Device	3	ES2
Control the subset of products through a control system, including access management and configuration.	Basic and above	Industrial	Both	1	
Implement strong authentication mechanisms for critical operations.	Substantial and above	All	Both	6	ES2
Implement session timeouts to limit the risk of user access compromising	Substantial and above	All	Both	4	
Integrate mechanisms for secure change of ownerships on the product.	Substantial and above	All	Both	2	
Require strong authentication and/or physical interaction with the product at the commissioning of the product	High	All	Both	1	ES2

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

The need for reliable identity and access management on ICT products is also essential, as identity-theft is a common vector of breach. However, ICT products, and especially IoT devices, do not always have the necessary mechanisms to protect the access on the device (for example, a study on popular smartwatches showed that only half of them would allow for a screen lock and access via PIN or pattern, sometimes with no protection against account enumeration[261]). Implementing the necessary mechanisms to ensure that the user access is proven and reliable, and as well as the identities of the services used by the products to function, especially as hardcoded password remain common (still present in 7% of Industrial Control Systems[262]).

4.2.2.4 Security requirements primarily associated with Essential requirement 4

Table 44 shows the security requirements primarily associated with Essential requirement 4 – Protect data and user's privacy.

Table 44 Security requirements primarily associated with Essential requirement 4

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Protect and encrypt traffic using secured protocols.	Basic and above	All	Both	13	
Secure the data at rest following state of the art standards on the matter.	Basic and above	All	Both	11	
Follow privacy regulations such as GDPR and inform the user about its privacy when using the service.	Basic and above	All	Both	9	ES5
Remove data on devices and services once the product/service is no longer used by the user or if the service is longer provided.	Basic and above	All	Both	7	

[261] Internet of Things Security Study: Smartwatches, HP, 2015

[262] industrial control systems vulnerabilities statistics, Kaspersky Labs, 2015

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Rely on external systems and platforms which guarantee an adequate level of security for the data and product.	Basic and above	All	Service	6	
Validate the integrity and security of data transferred by and to the product and protect against execution of data memory in compute resources.	Substantial and above	All	Both	10	ES2
Analyse output data to detect anomalies.	High	Industrial	Service	3	ES7

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

Data protection is a sine-qua-none condition in the usage of products and services by consumers, as surveys show that 81% of them would stop engaging with a brand online following a data breach, and 63% expect companies to be always responsible to protect their data[263]. ICT products must therefore meet these expectations ensuring by data is protected at all time, both in transit and at rest. Moreover, the privacy of the user data should remain at a high level throughout the usage of the product, including once the product is not used anymore (as research chooses that it is still possible to recover texts/chats on 85% factory wiped smartphones, and that in 25% of disk drives can be resold without any deletion method applied[264]).

4.2.2.5 Security requirements primarily associated with Essential requirement 5

Table 45 shows the security requirements primarily associated with Essential requirement 5 – Raise awareness to ensure a secure usage of the product in its context.

Table 45 Security requirements primarily associated with Essential requirement 5

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Provide clear information to the customer if the product requires additional configuration to be secure.	Basic and above	All	Both	5	ES1
Notify the user before the purchase on how long security updates will be provided.	Basic and above	All	Both	1	ES8
Provide training and configuration profiles to customers so that they can easily adapt the configuration to their risk scenarios and context.	Substantial and above	All	Both	5	ES1

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

As the general public remain the stakeholder who ultimately will manage the device for a large part of its lifecycle, it is key to ensure that he/she will have the necessary knowledge and skills to operate the product securely. While public authorities are increasingly releasing security guidance regarding IoT security for end users[265], each product

[263] Annual Survey, Consumers Hold Companies Responsible for Data Protection, Press Release, Ping Identity, 2019

[264] Smart Devices & Secure Data Eradication: the Evidence, WRAP, 2020

[265] Cybersecurity Awareness in IoT Threats, Mehrdad Sharbaf, IEEE, 2020

should provide the customised information which allows a secure usage in the users' context, as well as information on the period for which security updates will be provided.

4.2.2.6 Security requirements primarily associated with Essential requirement 6 – Ensure the resilience of the product and associated services

Table 46 shows the security requirements primarily associated with Essential requirement 6 – Ensure the resilience of the product and associated services.

Table 46 Security requirements primarily associated with Essential requirement 6

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Design products so that the service is able to sustain outages in data or networks.	Basic and above	All	Device	8	ES1
Define procedures and models to increase time to recovery for ICT products and services.	Substantial and above	All	Both	7	
Implement backup mechanisms to protect local data in case of compromising.	Substantial and above	Transport, Industrial	Both	4	ES4, ES7
Ensure a manual override mechanism is available for safety-related operations, in case a software-related issue was threatening the safety of a user.	Substantial and above	All	Device	3	
Provide determinist output if normal operations can be performed.	Substantial and above	Industrial	Both	1	
Design and implement resilient power systems.	High	Transport, Industrial	Both	5	

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

As ICT products are more and more present due to the ever-growing digitalisation of the society, they also tend to appear more often in critical contexts, such as medical environments, or energy production (evidenced by the investments in smart grids[266]). For example, in contexts in which incidents can affect the security of safety of humans, mechanisms should be introduced to ensure the continuity of the service provided by the ICT product, such as backups, resilient power systems or manual override to avoid accidents in case of remote takeover[267].

4.2.2.7 Security requirements primarily associated with Essential requirement 7

Table 47 shows the security requirements primarily associated with Essential requirement 7 – Detect security events and react to security incidents.

[266] Smart grid projects outlook 2017, JRC, 2017

[267] Black Hat USA 2015: The full story of how that Jeep was hacked, Kaspersky, 2015

Table 47 Security requirements primarily associated with Essential requirement 7

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Detect security anomalies, set up alerts and define response procedures to block attacks and intrusions.	Basic and above	All	Both	11	
Register the actions performed on the data plane and on the management plane.	Basic and above	All	Both	8	
Notify the user in case of critical operations performed on the device or service (credential changes, shutdown, etc.)	Basic and above	All	Both	1	ES5
Notify customers and third parties in case of breach or significant risks.	Basic and above	All	Both	1	ES5
Implement mechanisms to limit brute-force and DoS based attacks (throttling, timeouts, DDoS Protections, etc.)	Substantial and above	All	Both	6	ES6
Enable mechanisms to isolate the product from its network in case of network or product compromising.	Substantial and above	All	Both	3	ES6
Include remote deactivation/shutdown features.	Substantial and above	Transport, Industrial	Both	1	
Verify the integrity of the firmware already present on the product to detect potential compromising.	High	All	Device	4	ES8
Onboard automatic defence mechanisms within the product so that quick actions are taken in case of attacks.	High	All	Both	1	

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Even if the product has been adequately secured, it will still face attacks and threats, especially if connected to large networks or to Internet (as millions of hosts are scanning for vulnerable devices[268]). It is therefore important to ensure that ICT products are able to alert users and service providers in case of attacks, to enable investigation of attacks through appropriate logging of information and to notify users in case of breach or critical operations performed. However, as mentioned by stakeholders during the study, the logging detection features should be present within the limit set by the protection of user information and should not lead to less privacy for the customer.

4.2.2.8 Security requirements primarily associated with Essential requirement 8

Table 48 shows the security requirements primarily associated with Essential requirement 8 – Continuously evaluate and improve the security of the product.

[268] An Internet-Wide View of Internet-Wide Scanning, Zakir Durumeric, Michael Bailey, J. Alex Halderman, 2020

Table 48 Security requirements primarily associated with Essential requirement 8

Security requirement	Targeted risk profile	Sectors addressed	Targets Device or Service	Number of standards[255]	Other ERs addressed[256]
Update the firmware and software and fix vulnerabilities through updates (either automatic or through notification to the user).	Basic and above	All	Device	12	ES2
Define a process for vulnerability management and patching for all components (both hardware and software).	Basic and above	All	Both	10	ES2
Verify the integrity of received updates before installation using signature.	Basic and above	All	Device	9	
Maintain an inventory of the technologies and third-party software used on the product and services.	Basic and above	All	Both	6	
Train the staff that they will manufacture and operate the product and product services to ensure the security of the product from the provider side.	Basic and above	All	Both	5	
Onboard and train the top-management on cybersecurity so that it is considered across the organisation supporting the product.	Basic and above	All	Both	4	
Define a target operating model for cybersecurity assigning roles and responsibilities for the entire product lifecycle.	Basic and above	All	Both	4	ES1
Clarify the division of responsibilities between provider and user.	Basic and above	All	Both	0	ES5
Define mechanisms to securely decommission software or hardware technologies and subcomponents used within the product.	Substantial and above	All	Both	3	
Anticipate cybersecurity retrofitting needs while designing the product.	Substantial and above	All	Device	0	
Implement Information Sharing Agreements or open-source Vulnerability Disclosure procedures to enable vulnerabilities to be reported even if the product is not produced anymore.	High	All	Both	6	ES5

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Finally, as threats and vulnerabilities are constantly evolving, the product security must be continuously evaluated and improved during its lifetime. Several security functionalities must be present during the lifecycle, such as the ability to update the product (as such mechanisms are expected to be more commonly available[269]), the maintenance of an inventory of the technology used within the product, and a vulnerability management strategy (including for supply chain and hardware/software providers). Additionally, the staff involved with the making and operating of the product should be trained.

[269] Koen Zandberg, Kaspar Schleiser, Francisco Acosta, Hannes Tschofenig, Emmanuel Baccelli. Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check. IEEE Access, IEEE, 2019, 7, pp.71907-71920. ff10.1109/ACCESS.2019.2919760ff. ffhal-02351794f

4.2.3 Success factors

During the focus groups and interview led, the stakeholders shared best practices that might help with introducing and implementing the security requirement to the community. The suggestion shared are listed in Box 4.

Box 4 Suggestions for supporting the implementation of security requirements

- Increase the culture of information sharing, either:
  - through company culture (to raise the security level of the field all together);
  - through Information sharing agreements; and
  - through exchange groups (such as the economic interest group SECURITY MADE IN.LU in Luxembourg).
- Participate or manage platforms to help keeping up with product security (providing standard releases, technical reviews on technologies or attacks, etc.).
- Increase commitment from senior management in securing product.
- Provide incentive to share information regarding attacks and provide transparency on the product.
- Present certification as a positive item which can provide an assurance that security was considered in the making of the product, which can also serve as proof of non-liability should a security incident occur to the product.
- Ensure that the suppliers are aligned and include security in their product/component lifecycle. This will enable security to grow across the whole value chains (such as the Charter of Trust initiative[270], which invites company to comply with key principles such as "Ownership for cyber and IT security" or "Responsibility throughout the digital supply chain").

4.3 Conformity assessment procedures

Another part of the study aims at studying the conformity scheme procedures available to assess the fulfilment of the Essential Requirements. As the security requirements are more granular and verifiable, they can be used as assessment items to ensure that the Essential Requirements are fulfilled.

To do so, the following activities were performed:

1. A Desk Research was conducted to identify relevant certification schemes and assessment methodologies which can be used to evaluate the cybersecurity of ICT Products.
2. A Focus Group on Cybersecurity Activities was led to identify the relevant activities that can be used to assess the cybersecurity of ICT Products through the product lifecycle.
3. Interviews were conducted with Subject Matter Experts to complement the view on the current assessment methodologies.
4. Two data analysis were performed on two datasets to identify the need of each assessment activity for each risk profile:

[270] Information available at : http://www.charteroftrust.com/

- An analysis on the presence of assessment activities in certification schemes (Data Analysis #1), based on the data of Eurosmart Study "*A Cartography of Security Certification Schemes/Standards for IOT*"[271].
- An analysis on the possibility to use each assessment activity to assess the security requirements (Data Analysis #2).

As mentioned above, a data analysis was conducted to assess the presence of assessment activities in the certification schemes identified through the Desk Research. The certification schemes chosen aim to cover a large scope of products, although some of them might be used for a specific type of product (such as the Security Evaluation Standard for IoT Platforms addressing Internet of Things) or a specific sector (such as the IEC 62443 series of standards which address industrial equipment). The complete list of certification schemes in scope is provided in Table 51. This analysis aims to identify the "macro" activities present in certifications scheme and identify the most frequent ones for each risk profile. However, it should be noted that the review of certification schemes was done to gather information on assessment methodologies only and does not mean that all ICT Product should be certified.

4.3.1 List of assessment activities

Through the desk research, five assessment activities were identified. They are listed in Table 49. The activities are also mapped against the two phases mentioned in the Blue Guide[272] (Design phase and Production phase) in order to help alignment with current conformity assessment mechanisms. However, a third phase was introduced, to ensure that the security of the product once placed on the market is also assessed.

The importance of the organisational review was highlighted during the interviews, in which participants pointed out that the maturity of a provider/manufacturer should also be assessed in addition to the security present on the product, and that it could be the main type of review to perform in order to assess the products issued by very small companies with low security means. They also pointed out for the need to evaluate the security level of the supply chain and to require suppliers to also be assessed in terms of security. Another point which was made was that some security features are not useful unless the necessary support functions (organisational processes) exist to provide the necessary added value. One example provided was the need for security update mechanisms, which could end up being counter-productive if no solid vulnerability management and secure software development capabilities were present within the structure of the manufacturer updating the product.

Table 49 Identified conformity assessment activities

Assessment activity	Purpose	Phase(s) in which the activity take place	Assessment example	Presence in standards
Design review	Evaluate the initial design of the product and the mechanisms in place to ensure the security of the product.	Design phase	• *Architecture review* • *Network flow review* • *Logical architecture analysis* • *Etc.*	*OWASP ASVS, IEC 62443, TL9000, API STD 1164, etc.*

[271] Information available at : https://www.eurosmart.com/wp-content/uploads/2020/02/2020-01-27-Eurosmart_IoT_Study_Report-v1.2.pdf

[272] The 'Blue Guide' on the implementation of EU products rules, European Commission, 2016

Assessment activity	Purpose	Phase(s) in which the activity take place	Assessment example	Presence in standards
Code and configuration review	Evaluate the expected security baseline of the product in its final state before it is purchased.	Production phase	• *Software code review* • *Bug review* • *Sanitisation tests* • *Parameter reviews* • *Etc.*	*UL 2900-2-1, OWASP ASVS, IEC 62443, etc.*
Functionality testing	Evaluate the functioning of the main security/safety features present on the product.	Production phase	• *Feature tests on security functions and alerts* • *Resilience tests* • *Stress test* • *Etc.*	*OWASP ASVS, IEC 62443, API STD 1164, etc.*
Security testing	Identify potential vulnerabilities on the product or on the services supporting the product.	Production phase	• *Black box tests* • *Grey box tests* • *White box tests* • *Bug bounties* • *Hardware hacking* • *Data leak tests* • *Etc.*	*UL 2900-2-1, OWASP ASVS, NIST SP-800-115, API STD 1164, etc.*
Organisational review	Evaluate the ability of the organisation to support the security of the product.	Design phase Production phase Usage phase	• *Documentation review (procedures, processes, certifications etc.),* • *Interviews* • *Site visits* • *Staff evaluation* • *Supply chain review* • *Threat modelling review* • *User guidance review* • *Etc.*	*ISO 27001, UL 2900-2-1, IEC 62443, TL9000, API STD 1164, etc.*

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Moreover, the identified assessment activities were mapped against the conformity assessment activities as defined in the ISO 17067 standard[273], in order to ease the connection with other industry standards. The mapping is presented in Table 50. The definition of activities is defined in the ISO 17000 standard.[274]

Table 50 Mapping between Assessment activities and ISO17067 Conformity assessment activities

ISO 17067 Conformity assessment activities Study Assessment activities	Testing	Inspection	Design appraisal	Assessment of services or processes	Other determination activities[275]
Design review			✓		
Code and configuration review	✓[276]	✓			
Functionality testing	✓				Validation
Security testing	✓[276]	✓			
Organisational review				✓	Verification, Audit

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

[273] ISO (2013). Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes.

[274] ISO (2020). Conformity assessment — Vocabulary and general principles.

[275] Other conformity assessment types as defined in ISO 17000, but not explicitely listed in ISO 17067

[276] Notably in the context of automated tests, such as automatic code review or automatic penetration tests via tools.

The mapping between the assessment activities of the study and of the Conformity assessment as defined in ISO 17067 evidences that the combination of the study assessment activities covers the typical activity found in product assessment. Nonetheless, some assessment activities are difficult to distinguish between testing and inspection, notably to the addition of software assessment. Indeed, the security of the software can be evaluated in multiple way, whether it is through procedures, detailed requirements or on the basis of professional judgement.

To conduct the data analysis, some hypotheses are taken to classify the certification schemes and their associated level of conformity with the risk profiles. This hypothesis was used in order to provide a nuanced view on the importance of each activity for a given risk profile. The target risk level was identified based on the information available about the certification schemes, as well as on the preliminary assessment made in the Eurosmart study[271]. The classification is presented in Table 51.

Table 51 Certification schemes used for the Data Analysis #1

Certification scheme	Owner	Product addressed	Target risk profile	Corresponding certification scheme level
BSPA	AIVD/NLNCSA	All	Basic	/
CSPN	ANSSI	All	High	/
e-IoT-SCS	Eurosmart	Internet of Things	Substantial	/
LINCE	CCN	All	Basic	/
			Substantial	Basic + MCF
			High	Substantial + MEC
SOG-IS	SOG-IS	All	Basic	EAL1 / EAL2
			Substantial	EAL3 / EAL4 / EAL5
			High	EAL6 / EAL7
TÜViT-SQ	TÜViT	All	Basic	SEAL1
			Substantial	SEAL2 / SEAL3
			High	SEAL3 / SEAL4
BSZ	BSI	All	Substantial	/
IEC 62443	ISA	Industrial equipment	Basic	SL1 / SL2
			Substantial	SL3
			High	SL4
UL 2900	UL	Internet of Things	Substantial	/
SESIP	GlobalPlatform	Internet of Things	Basic	SESIP1
			Substantial	SESIP2 / SESIP3 / SESIP4 / SESIP5

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

It was also advised to look into the work done by ETSI TC Cyber, which should release by the end of the year a new an intermediate version of its standard on IoT Security (draft TS 103701 Vers. 0.5).

4.3.2 Mapping of assessment activities and risk profiles

Based on Data Analysis #1, the studies asses the presence of each assessment activity for a risk profile. The results are presented in Table 52 . Based on the analysis, the preliminary conclusions are listed below:

1. **Most certifications schemes**, regardless of the level, w**ill mandate a high-level design review and a penetration test.** The high-level design review is present in two third of certification schemes targeting basic risk profiles, and in all certification schemes targeting substantial and high risk profiles.
2. **Activities** between certification schemes targeting **substantial and high-risk profiles are rather similar.** For each activity, the difference between the presence of activities in certification schemes targeting substantial or high risk profiles remains within 10% of difference (besides for the code and configuration review, which is present in 57% of certification schemes targeting substantial risk profiles and 90% of certification schemes targeting high risk profiles).
3. **Functionality testing** and **organisational review** are **consistently less present** in schemes than other activities. Functionality testing are consistently present in around 40% of certifications of assessment schemes regardless of their targeted risk profile. On the other hand, organisational reviews are not performed for basic risk profiles and are present in less than half of the certification schemes targeting substantial and high risk profiles.

Table 52 Presence of assessment activities for each risk profile based on Data Analysis #1

Assessment activity		Targeting basic risk profile	Targeting substantial risk profile	Targeting high risk profile
Design review	High-level design review	67%	100%	100%
	Low-level design review	20%	92%	90%
Code and configuration review		20%	57%	90%
Functionality testing		40%	37%	40%
Security testing		83%	100%	100%
Organisational review		0%	42%	33%

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW

Based on Data Analysis #1, **a provisional mapping of activities** per risk profiles was developed. Some **assumptions** were taken into account to build the mapping:

- The **following values** were chosen for the mapping:
  - Activities present in 40% or less of certification scheme for a given risk profile are considered **optional**. Optional activities are activities which brings limited value in the assessment of a risk profile and does not address many requirements in scope for the risk profile.
  - Activities present more than 40% but 80% or less of certification scheme for a given risk profile are considered **recommended**. Recommended activities are activities which brings value in the assessment of a risk profile and addresses many requirements in scope for the risk profile.
  - Activities present more than 80% of certification scheme for a given risk profile are considered **mandatory**. Mandatory activities are activities which must be performed to ensure the security of the product, and addresses the majority of requirements.
- **The activity cannot be retrograded in terms of importance** (for example: a recommended activity for a basic risk profile cannot be optional for a substantial or high risk profile).

A first mapping was conducted based on these assumptions and is presented in Table 53. However, it was amended based on stakeholders' feedback obtained during the Focus Groups and Interviews (see Table 54Table 79 List of

ICT products classified by common categories – Energy (Smart grid)). Notably, the organisational review need was increased for all risk profiles due to the fact that the impact of organisational security aspects (e.g. supply chain security, cybersecurity awareness, usage of risk assessment, etc.) on the overall security of the products was consistently mentioned as a key aspect to consider. Also, the presence of "*Assessment of services or processes*" as a conformity assessment activity in ISO 17067 for product conformity assessment was considered as an additional argument to increase the importance of organisational review.

Therefore, the following changes were performed:

- The expected level of organisational review for basic risk profiles was changed to Recommended
- The expected level of organisational review for basic risk profiles was changed to Mandatory

The updated version of the mapping is available in Table 54.

Table 53 Initial mapping of activities based on data analysis

Assessment activity		Targeting basic risk profile	Targeting substantial risk profile	Targeting high risk profile
Design review	High-level design review	Recommended	Mandatory	Mandatory
	Low-level design review	Optional	Mandatory	Mandatory
Code and configuration review		Optional	Recommended	Mandatory
Functionality testing		Recommended	Recommended	Recommended
Security testing		Mandatory	Mandatory	Mandatory
Organisational review		Optional	Recommended	Recommended

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Table 54 Amended mapping of activities based on stakeholders' feedback

Assessment activity		Targeting basic risk profile	Targeting substantial risk profile	Targeting high risk profile
Design review	High-level design review	Recommended	Mandatory	Mandatory
	Low-level design review	Optional	Mandatory	Mandatory
Code and configuration review		Optional	Recommended	Mandatory
Functionality testing		Recommended	Recommended	Recommended
Security testing		Mandatory	Mandatory	Mandatory
Organisational review		Recommended	Mandatory	Mandatory

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

The participants of the Second Workshop challenged the final results of the mapping:

- Some participants pointed out that assessment activities are too strong for basic risk profiles as certification schemes usually apply to higher risk profiles, and that the certification schemes classified as basic for the data study reflect this view. They also mentioned that the scalability of the assessment schemes should be taken into account in the way activities are assessed as well.
- Additionally, one participant pointed out that comparing certification schemes as such might be misleading as they do not aim to certify the same products.

- Participants also pointed out that penetration tests are not consistent in quality and depth depending on the time spent on the exercise, which could lead to inconsistent results during the assessment phase. Their presence in certification schemes could also be influenced by the economic incentive to include a human, billable resource to justify or raise the price of the certification.
- Some participants also pointed out that even if some assessment activities were marked as optional or recommended, they should still be performed as some regulations could mandate it (such as GDPR mentioning Security and Privacy by Design).

During interviews, participants pointed out that the usage of certified, accredited third-party to conduct assessment was usually the preferred option to conduct conformity assessment, and that SMEs will most often need to rely on external certification bodies to assess the security of their product. However, one stakeholder noted that, above a certain project size, the added value of an external assessment would lower, due to two factors:

- As the certification body can intervene for long periods, it will work closely with the manufacturer teams for a long period, and therefore will have some connections with the people involved in the making of the product.
- It is sometimes more efficient to rely on internal teams which have an important knowledge the product to assess the security of the product (a newcomer could use much more time to reach the same quality of evaluation).

The most important point is that the team that assesses the product cannot be by any mean the one participating in the development of the product, nor report to the same entity, and cannot provide advice on how to improve the security, but only produce security findings. An example of such a model is the Project Zero[277] of Google, which aims to find zero-days in Google's systems as well as on commonly used technologies and website. However, they do not participate in the resolution of the vulnerability they identify.

[277] Information available at : https://googleprojectzero.blogspot.com/

5 Identification of policy options

The drive towards ubiquitous connectivity and digitalisation is increasing the diffusion of information and communication technology (ICT) products. Businesses, governments, and consumers are increasingly relying on these products for their everyday life and operations. According to the latest OECD Digital Economy Outlook, Internet usage has significantly increased over the last decade. In 2019 the proportion of adults accessing the Internet ranged from over 95% to less than 70% among OECD countries. Smartphones have also become the favoured device for Internet use in many countries: 75% of individuals in the European Union used a mobile phone or smartphone to connect to the Internet in 2018, up from 65% just two years earlier. Indeed, mobile broadband subscriptions increased in the OECD from 32 subscriptions per 100 inhabitants in 2009 to almost 113 subscriptions per 100 inhabitants by June 2019. The average mobile data usage per subscription in the OECD has quadrupled since 2014, reaching 4.6 GB in 2018. Machine-to-machine embedded mobile cellular subscriptions grew by over 21% in 2017-18. Furthermore, many countries in the EU are moving towards high-capacity fixed networks (Gigabit networks), and the next generation of wireless networks, i.e. 5G. [278] However. it is important to mention that today's IT systems are extremely complex: the Systems on a Chip of current smartphones have more than 8 billion transistors and current operating systems have more than 50 million lines of code. Many of these systems are built from parts supplied by many hardware and software vendors: this complexity makes more challenging securing the supply chain.[279]

Indeed, as shown by the recent SolarWinds incident, the software supply chain attacks represent "some of the hardest type of threats to prevent because they take advantage of trust relationships between vendors and customers and machine to machine communication channels such as software update mechanisms that are inherently trusted by users."[280] In the SolarWinds incident, a nation-state hacker group, compromised the infrastructure of SolarWinds, a company that manages a network and applications monitoring platform called Orion, gaining access to the platform and distributing trojanized updates to the software users. According to FireEye, one of the cybersecurity company that was object of this breach, the compromised plug-in of the Orion platform, "after an initial dormant period of up to two weeks, it retrieves and executes commands that allow to transfer files, execute files, profile the systems, reboot the machine, and disable system services."[281] All this activity was blended with legitimate SolarWinds activity and for this reason was difficult to detect. The New York Times, reported that this hacking, have affected more than 250 federal agencies and businesses in the USA but that SolarWinds ignored basic security practices and it has moved software development to Eastern Europe because it is cheaper, without considering that in this geographic area the nation-states intelligence is more influent.[282] Recently, also four zero-days vulnerabilities in Microsoft Exchange Server Software were actively exploited by state sponsored threat groups for various purposes such as steeling data from financial institutions. While patches have been provided by Microsoft, users that have not installed these could remain at risk.[283]

[278] OECD (2020), OECD Digital Economy Outlook 2020, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en.

[279] Lorenzo Pupillo (2019), 5G and National Security, CEPS, June. Available at: https://www.ceps.eu/5g-and-national-security//

[280] Constantin L. (2020), SolarWinds attack explained: And why it was so hard to detect", CSOonline

[281] Ibid.

[282] Sanger D. et al (2021), As Understanding of Russian Hacking Grows, So Does Alarm, The new York Times, 2 January

[283] Osborne C. (2021), Everything you need to know about the Microsoft Exchange hack, Zero Day, 19 April

Furthermore, the trend towards ubiquitous connectivity will increase with the diffusion of the Internet of Things (IoT). On the consumer side, IoT will make traditional goods increasingly "smart". Wearable products, home applications, toys and children equipment, cars, embedded with hardware and software will have the ability to connect. On the business side, IoT techniques will support a broad range of business innovations that will allow companies to integrate sensing, analytics and automated control into business models, reducing costs, improving productivity, customer services and overall performances, thus generating was has been called the "Industrial Internet".[284] The diffusion of "smart things" will soon outnumber computers and, in the near future, mobile phones too. According to the latest IDC forecast, the growth in connected IoT devices is expected to reach 41.6 billion units by 2025 and generating 79.4 zettabytes of data[285] while the global IoT market value market is anticipated to reach US$ 1,102.6 Bn by 2026 at a CAGR of 24.7% during the forecast period (2019 - 2026).[286]

However, all smart products – being them software-based – are vulnerable to digital security threats. Software weaknesses allow an attacker to compromise the integrity of the product and exploit it. Many companies producing "smart things" today are not specialised in security. With the increase of the attack surface, the occurrence of security incidents is growing. Whilst this could ultimately generate a lack of trust in the online environment and fears for privacy violations in consumers, from a business perspective, the effects of the situation described above could be registered in the smooth functioning of production lines. Nevertheless, the most feared threat is for the physical safety of users.

In the context of this Study, the chapter will explore and suggest policy options for identifying the most appropriate intervention by the policymakers for addressing the rising cybersecurity risks in the use of the ICT products.

The policy options presented in this chapter have been designed based on the EC terms of reference of the project, an extensive literature review and desk research, close reference to the NLF as a toolbox for product legislation, five interviews with the governments of Finland, Germany, the Netherlands, UK and Japan, conducted in November 2020, and 14 interviews with companies, Industry and consumer organisations and Competent Authorities conducted in January 2021.

Figure 33 presents an overview of the policy options, differentiated according to their nature:

1. *Voluntary measures,*
2. *Regulatory measures.*

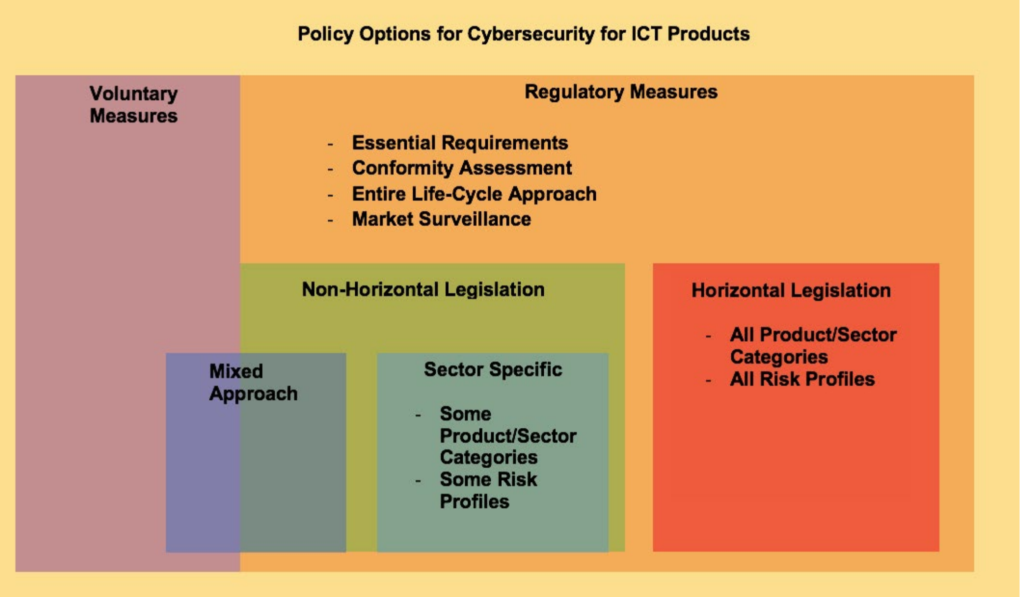
The *Regulatory measures,* while always entailing some specific policy actions such as essential requirements, conformity assessment, entire lifecycle approach and market surveillance, can be applied **to all** product/ sector and risk profiles (***Horizontal legislation***) or **some** product/sector categories and risk profiles only (***sector-specific***). A *Mixed approach* policy option – combining regulatory and voluntary measures – has also been taken into consideration.

[284] OECD (2015), Internet of Things: seizing the benefits and addressing the challenges, OECD Digital Economy Policy Papers

[285] MacGilliv ray C. et al (2019); Internet of Things Ecosystem and Trends, IDC. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[286] IOT Industry Report (2020), Internet of Things Market Size, Growth | IoT Industry Report 2026

Figure 33 Overview of the Policy Options



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW

Table 55 presents the policy options at a glance. These will be discussed in more detail in the following sections.

Table 55 The policy options at a glance

Policy option 0: Baseline	Policy Option 1: Voluntary Measures	Policy Option 2: Horizontal Legislation	Policy Option 3: Sector-pecific Legislation	Policy Option 4: Mixed Approach
This policy option leaves business "as usual"	Current voluntary practices and measures to increase transparency and promote conformity assessment	Implementation of a common regulatory approach applicable to all categories and risk profile of ICT products	Implementation of a common regulatory approach applicable only to specific ICT products / risk levels or sectors	Implementation of a combination of regulatory and voluntary measures

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021)

5.1 Mapping NLF against the policy options

5.1.1 The NLF and Cybersecurity

As mentioned in the introduction to this chapter, the policy options have been designed with reference to the NLF. The NLF can be considered as a toolbox of measures for use in product legislation. In order to frame the different policy options, the Project Team has chosen to select the main measures provided by NLF and, followingly, evaluated how these could be applied to the field of cybersecurity for ICT products. In particular, the Project Team focused on the following: essential requirements, conformity assessment mechanisms, reference to standards and, finally, on the provisions for market surveillance.

Essential requirements

According to the NLF, *"essential requirements must be applied as a function of the hazard inherent to a given product. Therefore, manufacturers have to carry out a risk analysis to first identify all possible risks that the product may pose and determine the essential requirements applicable to the product. This analysis has to be documented and included in the technical documentation […].*[287] *Essential requirements define the results to be attained, or the hazards to be dealt with,* ***but do not specify the technical solutions for doing so****. The precise technical solution may be provided by a standard or by technical specifications or be developed following general engineering or scientific knowledge […]."*[288] The flexibility provided for by this measure allows manufacturers to choose the manner in which requirements are to be met. This approach is pivotal in the context of cybersecurity as it allows for an adaptation that takes into account the evolution of technology.

As far as cybersecurity for ICT Products is concerned, the NLF provision for essential requirements implies that the selected essential requirements must specifically mention which cybersecurity risk need to be addressed, while the **technical details** and further domain-specific measures are based on **harmonised standards** listed in the Official Journal of the EU.[289]

Conformity Assessment

Within the framework of the NLF, Decision No 768/2008/EC lays down the 'horizontal menu' of conformity assessment modules and the ways in which procedures are built. Following this Decision, the legislator can select – from the menu of conformity assessment modules and procedures – the most appropriate ones for the concerned sector. The reason for providing variants within modules is to "enable the necessary level of protection to be ensured for products presenting a higher level of risk while avoiding the imposition of a heavier module. The idea is to minimise the burden on manufacturers to the extent possible."[290] This applies for all variants of all modules laid down under Decision No 768/2008/EC.

In this context, the assessment of the risk associated with a product is a key concept that should nevertheless also be applied in the context of cybersecurity. Particularly, risk is considered as the result of the combination of impact and probability, considered under the condition of the product's intended use. This meets with the level of flexibility

[287] The manufacturer must draw up a technical documentation. The technical documentation is intended to provide information on the design, manufacture and operation of the product". Point 4.3 of the European Commission (2016), Commission Notice- The Blue Guide on the Implementation of EU Product Rules, Official Journal of the European Union, 26 July, p. 56

[288] European Commission (2016), Commission Notice- The Blue Guide on the Implementation of EU Product Rules, Official Journal of the European Union, 26 July, p.39

[289] "A harmonised standard is a European standard developed by a recognised European Standards Organisation: CEN, CENELEC, or ETSI. It is created following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation. The references of harmonised standards must be published in the Official Journal of the European Union." See: European Commission, Harmonised Standards (https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en)

[290] European Commission (2016), Commission Notice- The Blue Guide on the Implementation of EU Product Rules, Official Journal of the European Union, 26 July, p. 65

required in the context of cybersecurity as a product might be used differently depending on if they are placed in a critical infrastructure context or in a safe environment.

Reference to standards

The NLF refers to 'harmonised standards' in cases where standards are published in the Official Journal of the EU. **According to the NLF, using these standards would grant the manufacturer a presumption of conformity to the legislation.** Reference to standards makes legislation per se lighter and more flexible to reflect the evolution of technologies. This concept is thus particularly relevant to the context of cybersecurity for ICT products.

Market Surveillance

According to the NLF, market surveillance occurs at the marketing stage of the products. Market surveillance activities may be organised differently depending on the nature of the product and its legal requirements; activities may range from control of formal requirements to profound laboratory examinations. All economic operators have a role and obligations in market surveillance. Thus, market surveillance does not formally take place during the design and production stages, which is before the manufacturer has taken formal responsibility for the conformity of the products, usually by affixing the CE marking. However, nothing formally prevents market surveillance authorities and economic operators to collaborate during the design and production phase.

For market surveillance to be efficient, resources should be concentrated where risks are likely to be higher or non-compliance more frequent, or where a particular interest can be identified. In this context, if a product presents a risk to the health or safety of persons or other aspects of public interests, market surveillance authorities must request without delay to relevant economic operators to:

- take any action to bring the product into compliance with the applicable requirements laid down in the Union harmonisation legislation; and/or
- withdraw the product; and/or
- recall the product; and/or
- stop or restrict supplying the product within a reasonable period.

Economic operators must ensure that corrective action is taken throughout the EU. Market surveillance authorities must also inform the relevant body (if any) of the decision taken. In case of serious risk requiring rapid intervention, the market surveillance authority may adopt restrictive measures without waiting for the economic operator to take corrective action to bring the product into compliance.

In the context of cybersecurity for ICT Products, it should be noted that moving into the digital environment the concept of recall – here, 'digital recall' – might be more easily implementable as well as scalable. Indeed, software/firmware updates can be performed remotely for a large number of devices as long as they are connected.

5.1.2 Mapping the NLF against the Policy Options

The Project Team has envisaged five preliminary policy options:

- **Baseline:** This policy option leaves the situation unchanged; namely relying on the existing regulatory framework.
- **Voluntary measures**: This policy option relies on current voluntary practices and measures.
- **Horizontal legislation**: This policy option entails the implementation of a horizontal regulatory approach applicable to all categories and risk profiles of ICT products.
- **Sectors or product categories specific legislation**: This policy option envisages the implementation of legislation applicable only to specific ICT products categories or risk profiles.
- **Mixed Approach**: This policy can be understood as the implementation of a co-regulatory and regulatory approach based on specific categories and risk profiles of ICT products.

Based on the previous analysis of the NLF, these policy options – except for the Voluntary measures - can be better explained with the help of the NLF measures considered above (i.e. essential requirements for ICT products, conformity assessment mechanism, reference to standards, and the provisions for market surveillance).

Essential product requirements

The main aspects related to the product requirements envisaged in the NLF definition of essential requirements are relevant across three policy options: Horizontal legislation, Sectors or product categories' specific legislation and Mixed approach.

In this context, the concept stemming from the NLF is that the **manufacturer has full responsibility** for the product meeting the essential requirements. Hence, in case a manufacturer buys from a supplier a piece of software that is then integrated into his product, it is his responsibility to verify that after such integration the product still complies with the relevant legislation.

The issue lays in the fact that no cybersecurity requirements to comply with have yet been defined. Hence, the manufacturer is not obliged to comply with any specific cybersecurity provisions, although still liable for a damage caused by a security breach**.** Nonetheless, once such cybersecurity requirements will be issued, the responsibility of ensuring that cybersecurity requirements are met will continue to fall on the manufacturer.

In the context of Cybersecurity for ICT products, since it is required to address security through the entire lifecycle**, there is the need to envisage also post-market requirements in addition to pre-market requirements**. Furthermore, it is necessary to assess **how broad these requirements should be to factor in the different threat models and risks for the different sectors.** Finally, the notion of manufacturer would require further clarifications as, especially in the case of IoT, there might be cases in which the reseller could be considered as manufacturer of the product.

Conformity Assessment

As mentioned earlier, the NFL conformity assessment provisions offer a menu of different modules that are coherent with the different risk level of products. The NFL envisages three possibilities for conformity assessment: self-assessment, conformity assessment performed with the involvement of an accredited in-house conformity assessment body and finally, **third-party conformity assessment by an external conformity assessment body acting as an impartial and fully independent entity from the organisation or the product it assesses.** These possibilities could be used in framing the different policy options, as the body in charge of the conformity assessment might defer depending on the risk profiles or sector.

Market Surveillance

The NLF provisions for market surveillance are applicable to all different policy options considered in this study, with the exception of Voluntary measures. Specifically, in case of serious risk requiring rapid intervention, market surveillance authorities may adopt restrictive measures without waiting for the economic operators to take corrective actions.

In this context, particular attention should be dedicated to a **proper mechanism for the identification of competent authorities** taking care of the violation of the security requirements. According to consumer organisations and market analysts, the allocation of responsibilities among authorities results as not being clear at the moment.

Table 56 summarises the mapping of the NLF policy measures on the preliminary policy options introduced above.

Table 56 Preliminary Mapping of NLF against the policy options

Policy Options	NLF Measures				
	Description	**Product requirements**	**Conformity assessment**	**Accreditation**	**Market Surveillance**
Baseline	This policy option leaves "business as usual": Relying on the existing regulatory framework				
Voluntary measures	Current practices and measures – Industry led - to increase transparency and promote conformity assessment				
Horizontal legislation	Implementation of a common regulatory approach applicable to all categories and risk profiles of ICT products	Definition of essential requirements applied to all sectors/products. Harmonised standards.	Modules coherent with the risk level; Self-assessment and Conformity assessment performed by a third party	No difference	In case of serious risk requiring a rapid intervention, the market surveillance authority may adopt restrictive measures without waiting for the economic operator to take corrective action.
Sectors or product categories specific legislation	Implementation of legislation applicable only to specific sectors or product categories or risk profiles	Definition of essential requirements only for a specific set of products. Harmonised standards.	Modules coherent with the risk level. Self-assessment, and Conformity assessment performed by a third party	No difference	In case of serious risk requiring a rapid intervention, the market surveillance authority may adopt restrictive measures without waiting for the economic operator to take corrective action.
Mixed approach	Implementation of a Co-regulatory and regulatory approach based on specific categories and risk profiles of ICT products	Definition of a mix of requirements. Essential requirements for many sectors/products, and voluntary requirements for a group of products. Harmonised standards.	Modules coherent with the risk level. Self-assessment and conformity assessment performed by a third party	No difference	In case of serious risk requiring a rapid intervention, the market surveillance authority may adopt restrictive measures without waiting for the economic operator to take corrective action.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

5.2 Analysis of policy options

5.2.1 Analysis and specification of Policy Option "0": Baseline

Introduction

According to Tool #17 of the Better Regulation Toolbox,[291] the first step in the identification of the policy options is the establishment of a baseline; this functions as a benchmark from which the impacts of the various policy options can be measured. The Project Team has conventionally called this option Baseline, or Option 0. This policy option will be characterized as "no policy change scenario", implying that the situation is left as it is.

Specification of Policy Option: Baseline

The current situation of cybersecurity for ICT products in the EU is detailed below.

1. The Project Team has performed the analysis of the existing EU legislative framework with two aspects in mind: (i) type and levels of coverage for ICT Products, (ii) level of cybersecurity requirements present in the existing legislation. The analysis led to the identification of a set of regulations including all legislation that relates to theNLF, and legislation that has a strong link to the topics of cybersecurity and data protection (e.g., NIS Directive; eIDAS Regulation; General Data Protection Regulation). In performing the legislative gap analysis, the Project Team has performed a comparison of the requirements contained in 37 pieces of EU legislation against the cybersecurity objectives set by Art. 51 of the Cybersecurity Act. The latter was taken as a reference as it represents one of the most up-to-date piece of legislation concerning cybersecurity and providing a comprehensive set of requirements for products and services. The analysis revealed that the European legislative landscape is broad and comprehensive. However, it does not target ICT products specifically. More specifically, the following conclusions from the analysis are pointed out: (i) the current EU legislative framework does not cover all the security objectives set out in Art. 51 of the Cybersecurity Act; (ii) legislation related to the NLF does not address fully the cybersecurity requirements for ICT products; (iii) the granularity of some of the requirements identified in the legislation does not guarantee the fulfilment of the security objectives and; (iv) some cybersecurity requirements addressed to service operators apply indirectly to ICT products used to operate the service. At the same time, the analysis of national legislation shows that Member States – with some exceptions – are not planning to bring forward any legislative proposal that could enhance the cybersecurity of ICT products.

[291] European Commission (2021), Better Regulation Toolbox, https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why -and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en

2. The following legislative reviews are underway. These could impact the cybersecurity legislative landscape in the EU. In particular:

    a. Delegated Acts under the RED;

    b. The evaluation of the NLF;

    c. The review of the Directive on Security of Network Information Systems (the NIS Directive);

    d. The review of the General Product Safety Directive (GPSD);

    e. The review of the Machinery Directive (MD); and

    f. Several certification schemes under the Cybersecurity Act (CSA).

3. Cybersecurity threats to ICT products are increasing. According to ENISA, “the sophistication of threat capabilities increased in 2019, with many adversaries using exploits, credential stealing, and multi-stage attacks.” The cybersecurity agency highlighted five trends with cyber threats in 2020:[292]

    a. **Malware upgrade:** *“Malware family strains are being updated into new versions with additional features, distribution and propagation mechanisms. Emotet for example, a malware originally designed as banking Trojan back in in 2014, has become one of the most effective malware distributors of 2019”*

    b. **Threats will become fully mobile:** *“Users are increasingly dependent on mobile devices to secure their accounts. The use of 2fa tied to an app authenticator or via a text message is one of the examples. With more malware going full mobile, fraudulent apps or SIMJaking make these devices the weakest link and, therefore, extremely vulnerable to attacks.”*

    c. **Attackers are using new file types such as disc image files (ISO and IMG) for spreading malware**: *“DOC, PDF, ZIP and XLS files are still the most commonly used attachment type for spreading malware but other types are getting popular. A few campaigns distributing AgentTesla InfoStealer and NanoCore RAT were found using image file type in 2019.”*

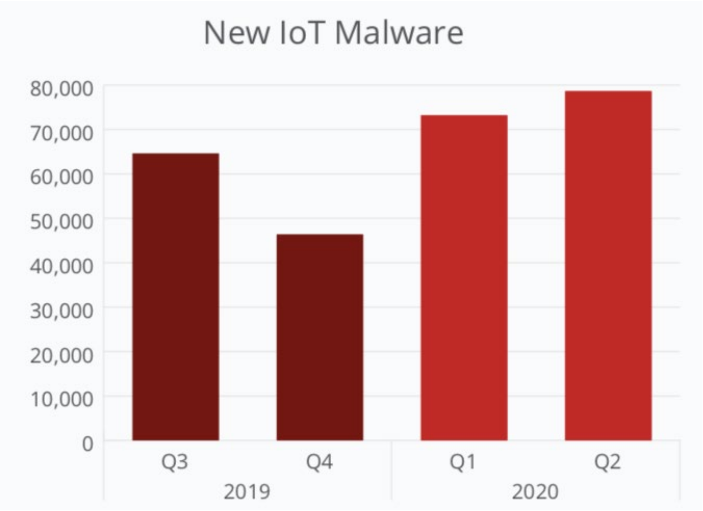
    d. **Increase in targeted and coordinated ransomware attacks:** *“In 2019, we saw an escalation of sophisticated and targeted ransomware exploits with the public sector, health care organisations and specific industries at the top of the list. Attackers are spending more time gathering intelligence about their victims, knowing exactly what to encrypt, achieving maximum disruption and higher ransoms.”*

    e. **Credential-stuffing attacks will widespread:** *“Credential stuffing - the automated injection of stolen username and password combinations through large-scale automated login requests directed against a web application - will proliferate as a result from a decade of an abnormal number of data breaches and trillions of personal data records stolen.”*

[292] ENISA (2020), “Emerging Trends. ENISA Threat Landscape”, October. Available: https://www.enisa.europa.eu/publications/emerging-trends

4. Malware has made ENISA's list of top 15 threats."[293] In particular, as shown in Figure 34,IoT malware in 2020 increased 7% from 2019, due to Gafgyt (also known as Bashlite) and Mirai, two of the most common types of malware infecting IoT devices.

Figure 34 IoT Threats



SOURCE: MCAFEE LABS (2020)

5. The specific dynamics of ICT product markets. As mentioned in Chapter 1. The market for ICT products is characterized by specific dynamics that create a misalignment of incentives between the behaviour of economic operators and optimal levels of security. Indeed, since the ICT products contain software and the market for SW products is characterized by network economics with first-mover advantages ("we will ship on Tuesday and get it right on version 3.0"), this dynamic values cost-effectiveness, usability and time to market over security. Furthermore, even though the alignment of incentives could be corrected, the market for cybersecurity of ICT products could fail in delivering optimal levels of security given to information asymmetries and negative externalities.

Therefore, the "No Action" that characterises the baseline option would entail leaving the current "status quo" as it is now.

5.2.2 Analysis and specification of Policy Option 1: Voluntary Measures

Introduction

[293] ENISA (2020)," Main incidents in the EU and Worldwide. ENISA Threat Landscape", October. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

The concept of "ICT Product" is relatively new in the cybersecurity policy. Traditionally, policymakers and regulators in this area have concentrated their attention on the cybersecurity of organisations' information systems.[294] However, with the increasing role of digital connectivity in our society and in particular with the explosive growth of IoT devices that simultaneously increased both the attack surface as well as the number of vulnerabilities, policymakers started to pay more attention to the cybersecurity of specific categories of ICT products such as smartphones and more in general connected devices. According to the GSMA, the number of connected devices is already greater than the number of people on the planet and this figure is expected to reach 25 billion by 2025, a quarter of which will be in Europe.[295]

To start with, many governments have favoured voluntary approaches to ICT products security afraid that regulatory intervention could stifle innovation and competition. The fast-changing technological landscape of these markets played also a role, suggesting avoiding ex-ante regulation due to the quick obsolescence of the measures implemented.

Based on desk research and interviews with policymakers from the UK, Japan, Finland, Germany and The Netherlands, the following groups of **voluntary policy measures**, have been identified:

- Voluntary certification as defined in the Cybersecurity Act;
- Codes of Conduct;
- Government procurement policy;
- Awareness-raising campaigns;
- Commission recommendations; and
- Industry-led initiatives.

Voluntary certifications as defined in the EU Cybersecurity Act [296]

The EU Cybersecurity Act (CSA) encompasses a significant example of **voluntary conformity assessment** in the EU. The CSA envisages ICT certification at the EU level through a European Certification Framework for the establishment of voluntary European certification schemes. The goal of this process is twofold. First, to ensure an adequate level of cybersecurity for ICT products, ICT services and ICT processes by increasing security and trust in the certified products, services and processes. Second, to help to avoid the multiplication of conflicting and overlapping national cybersecurity certification schemes, reducing in this way the fragmentation of the internal market with regard to cybersecurity certification schemes. The cybersecurity certification process represents a win-win situation for the different stakeholders in the market. Products supplier using certification could show that their products have fulfilled specific requirements and that they are committed to providing secure products in the market.

[294] OECD (1992), Guidelines for the security of Information systems. Available: https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

[295] GSMA (2020), The internet of Things 2025. Available at: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf

[296] This section draws from; European Commission (2019), 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 on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

Customers could be more confident that the products they buy are more secure since they comply with specific security requirements.

The European cybersecurity certification framework lays down the main horizontal requirements for the development of the European certification schemes and allows for **European cybersecurity certificates** and **EU statement of conformity** for ICT products, ICT services and ICT processes. Starting with an EU Certification scheme that includes the cybersecurity requirements, the conformity assessment bodies, accredited by the national accreditation bodies, which are supported by the National Cybersecurity Certification Authorities, using a conformity assessment procedure certify the conformity of the product and release the **European cybersecurity certificate**.

The certification schemes allow also for a conformity assessment carried out under the sole responsibility of the manufacturer or provider of ICT, products, services or processes (**conformity self-assessment**). In this case, the process provides for an EU **statement of conformity.** This document states that the specific ICT product complies with the requirements of the European cybersecurity certification scheme and the manufacturer assumes responsibility for the compliance of the ICT products. Conformity self-assessment is usually considered to be appropriate for low complexity products characterized by low risk to the public (assurance level basic). For the other two assurance levels envisaged by the Cybersecurity certification schemes - substantial and high -, the evaluation process is conducted by a **third-party certification body** that, at the end of the process, releases the European cybersecurity certificate.

As envisaged by the CSA, the Commission is preparing with the support of the European Cybersecurity Certification Group 'ECCG' and the Stakeholder Cybersecurity Certification Group and through open consultation, a Union Rolling work Programme for European cybersecurity certification schemes. "The first Union Rolling Work Program will be adopted in the first quarter of 2021 and will allow industry, national authorities and standardization bodies to prepare in advance for future cybersecurity certification schemes" also for IoT.[297] Furthermore, the Commission is working with ENISA on the preparation of a candidate cybersecurity certification scheme (the EU-CC) to serve as a successor to the Senior Officials Group-Information Security (SOG-IS) Mutual Recognition Agreement, the first European model for cooperation and mutual recognition in the field of security certification that however, included only some Member States. Additional work is underway for the definition of a European certification scheme on Cloud Services (EU-CS).[298]

Open issues related to voluntary conformity assessment [299]

As mentioned previously, the conformity assessment has many positive aspects related to increasing security and consumers' trust in the products that follow this process. However, the conformity assessment raises also some concerns. The risk of non-compliance for **the self-assessment case** depends on the degree of market surveillance by the Member States. According to Blyte and Johnson,[300] some European Studies on the implementation of the

[297] European Commission (2020), The EU's Cybersecurity Strategy for the Digital Decade, p. 9

[298] See Andreas Mitrakas (2020), The EU cybersecurity certification framework: performance highlights", ENISA presentation at the Cybersecurity@CEPS Summit 2020, 2 December. Available at: https://www.ceps.eu/ceps-events/cybersecurityceps-summit-2020/

[299] This section draws from OECD (2021), "Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

[300] Blyte and Johnson (2018), Rapid evidence assessment on labelling schemes implications for consumer IoT security, PETRAS IoT Hub

energy labelling directive show that between 5%-40% of the electrical products were found for sale without the energy label and that the overall non-compliance rate with the directive was about 20%.

When it comes to **third-party certification** there are some concerns related to:

1. Costs: the certification process bears direct cost related to the services offered by the certification third-party and indirect cost related to the increased time to market.
2. According to Blyte and Johnson (2018), certification in the context of IoT will raise the issue of scalability: With billions of internet connected objects and consumers, on average, owning 15 connected products," this is challenging for any scheme that requires certification and significant pen-testing as it is costly and may not scale in a world of 20 billion connected things". Therefore, third-party certification may not be scalable to all IoT devices but should be used only for medium or high-risk products.[301]
3. Certification would probably help the advanced user to make better choices but will not be valuable for mainstream users that probably are not familiar with ISO standards unless the certification information is accompanied by information such as labels. more easily understandable to them.
4. Due to the dynamic nature of the ICT products that require continuous software updates, the certification process could be no longer valid after the update. Therefore, when certification is mandatory, it could become an obstacle to the security updating generating an "insecurity by compliance."[302]
5. Certification could hamper the competitiveness of EU companies in the international scenario where less stringent rules are imposed.

Labelling

Labelling can also be considered under the umbrella of voluntary certification. Labels on ICT products can be very helpful in reducing information asymmetries between sellers and buyers and in realigning market incentives among stakeholders. In particular, according to the OECD (2021b). using labels can help achieve the following objectives:

1. Show to the customer that the product has a given level of quality;
2. Inform the customer about the product characteristics in a simple and clear manner; and
3. Allow customer to compare different type of products.

Labels have quite different characteristics:

1. Can be mandatory as in the case of energy label in the EU or voluntary like in the case of "organic" food;

[301] The difficulty related to testing hundreds of IoT devices ("20 different CPU by 50 different manufacturers") has been also mentioned by Ross Anderson during the Panel on Cybersecurity for ICT Products at the Cybersecurity@CEPS Summit 2020 on the 2nd of December

[302] "Mandatory certification can lead to insecurity by compliance, as in Brazil where ISPs do not update some telecommunication equipment in order not to break mandatory certification requirements. Certification-related regulation needs to take economic aspects into account. It may not be economically feasible to certify everything on platforms that integrate many different parts. Risk-based approaches will be necessary to determine the components the certification of which can really bring value." OECD (2019), Summary Report of the Inaugural Event Global Forum on Digital Security for Prosperity, page 10. Available at: https://www.oecd-ilibrary.org/docserver/3206c421 en.pdf?expires=1608987015&id=id&accname=guest&checksum=B53B49F203539AE51BB6B03F541513F2

2. Can be issued by public authorities or industry associations;
3. Can provide simple information about the product such as a list of ingredients or be associated with a given level of quality (certified label); and
4. Are based on declaration or self-assessment (like in the energy label) or may require a specific validation by a third party.

The labelling system is quite developed in the energy and the food sectors and there is empirical evidence that, for instance, in the food sector the presence of labels increases healthy product choice by 18% indicating that labels do empower consumers to choose healthier food." Even the mere presence of a label may be beneficial, a phenomenon known as the "feature-positive effect" which suggests that seeing a label is more informative – and likely to influence consumer choice - than not seeing a label at all." Also, in the energy sector, research shows that "consumers are willing to pay more for energy-efficient products as rated by labelling schemes and around half of the citizens from ten European countries opt for Energy Labels as a key source of information to support purchasing decision making."[303] In Europe, labelling for ICT Products is already in use in Finland and Germany. Outside the EU in Japan.[304]

However, labels carry also a number of shortcomings. According to the OECD, labels tend to simplify a quite complex issue: while labels aim to facilitate consumers understanding of security, they could also "be misunderstood by mainstream users as a guarantee of full digital security, even though they only signal that the product fulfils certain requirements.[305] Furthermore, labels can generate consumer fatigue when customers are exposed to too many labels [306] and if not enough companies adopt the label, the impact of this system will likely be very limited.

In this respect, it should also be considered that ICT-products might be put into usages with variable security risks. In order to cater for this possibility, the labelling system should allow end-users to be informed of the intended usages for which the products' security was designed. The labelling scheme should thus be conceived in such a way to expressly warn users that the ICT product should be used only for certain specifically identified applications. Else, the label could attribute a colour scale to the products based on the envisaged use cases: from green (maximum security for all possible applications) to yellow (not secure for certain sensitive use cases) or red (least level of security).

According to an analysis performed by BEUC and ANEC, the information presented in the labels on the cybersecurity elements of the products risk creating confusion because of the technicality of the subject matter (e.g. information on the encryption system used may not speak to all consumers). As such, labels should be qualitatively tested to ensure that they are well designed and provide a level of information that is consisted with the expected digital literacy of end-users, such as that consumers can effectively understand the meaning of the label.[307]

[303] Blyte and Johnson (2018), Rapid evidence assessment on labelling schemes implications for consumer IoT security, PETRAS IoT Hub p. 5 and p. 8

[304] Manufacturers use physical labels to convey compliance in order to access markets. Physical or e-label are used to provide information on safety, electromagnetic interference, energy, materials, and/or recycling requirements. The use of Labelling to convey information on product security is a quite recent phenomenon and it is mostly focused on IoT devices.

[305] OECD (2021), "Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

[306] See Blyte and Johnson (2018)

[307] BEUC, ANEC (2019), Keeping Consumers Secure: How to tackle cybersecurity threats through EU law, November, p. 16

[2] Ibid.

Besides, if a label is not subject to a legal framework guaranteeing an adequate level of market surveillance is in place to check compliance with the label requirements, then the labelling scheme might be partially or completely ineffective. For this reason, as this study will mention when the policy option “mixed approach” will be presented, to be more effective, labels should be used in conjunction with ex ante regulatory measures,

Box 5, Box 6 and Box 7 offer an overview of the experiences of Finland, Germany and Japan. The interviews with the government of Finland and Germany revealed that these countries have promoted labelling schemes in anticipation of legislative measures at EU level. A more detailed analysis of the Labelling schemes in place in these countries can be found in Annex IV – Labelling.

Box 5 Labelling in Finland[308]

Labelling in Finland

The Finnish Transport and Communications Agency Traficom has implemented a program of Labels for IoT products. The program aims at helping consumers to make more secure choices when purchasing IoT devices or services. The label informs purchasers that the device or service has passed an audit phase, based on the security requirements set by the National Cyber Security Centre Finland NCSC-FI. Furthermore, the Cybersecurity Label helps producers in showing their commitment to IoT security. While the Finnish government would have welcomed a harmonized approach at the EU level, at the time of the implementation of the Cybersecurity Labels, no common mechanism was available.

To receive the label, a vendor must contact the NCSC-FI and fill in a statement of compliance form. Then, a threat model and a testing plan are crafted by the NCSC-FI. If the product passes the testing phase the certificate will be granted to the vendors.

The Finnish government has envisaged several security requirements that the vendors should fulfil to acquire the Cybersecurity Label. These requirements are mapped against the ETSI Standards:

1. Where passwords are used and, in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user (ETSI 5.1-1).
2. When the device is not a constrained device,[309] it shall have an update mechanism for the secure installation of updates (ETSI 5.3-2). An update shall be simple for the user to apply (ETSI 5.3-3). Updates shall be timely (ETSI 5.3-8). The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by the update (ETSI 5.3-11). The manufacturer shall make a vulnerability disclosure policy publicly available (ETSI 5.2-1). Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period (ETSI 5.2-3).
3. The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes and for each device and service. This also applies to third parties that can be involved, including advertisers (ETSI 6.1).
4. Sensitive security parameters in persistent storage shall be stored securely by the device (ETSI 5.4-1). The consumer IoT device shall use best practice cryptography to communicate securely (ETSI 5.5- 1). The manufacturer shall follow secure management processes for critical security parameters that relate to the device (ETSI 5.5-8).
5. Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practices on usability (ETSI 5.12-1).

[308] This section is based on the interview with the government of Finland on the 8th of December 2020

[309] Defined as: "Category of connected devices with stringent resource restrictions compared to common desktop computers, such as (i) significantly reduced power consumption, (ii) much less computation power or (iii) orders of magnitude less memory. Furthermore, constrained devices are typically based on micro-controllers that provide only a limited set of functionalities e.g., they are typically not equipped with memory management units, which de facto rules out using operating systems such as Linux on such devices. The IoT is currently held back by fragmentation due to a plethora of too rudimentary, and too hardware-specific software platforms, employed on constrained devices to accommodate network stacks and applications. Only recently is progress being made in this domain with the emergence of new operating systems which aim to provide an open source, modern, generic software platform upon which one can conveniently build IoT application software." Hauke Petersen, Emmanuel Baccelli, Matthias Wählisch (2014), "Interoperable services on constrained devices in the internet of things.", June.

Labelling in Finland

Since most Finnish companies are SMEs, the government first considered establishing self-assessment procedures. However, vendors participating in the pilot of the Cybersecurity Label advocated for having the evaluation performed by a third-party. The cost of the inspection depends on the amount of work and the pricing of the inspection body, which have the right to price their work independently. Besides, the testing costs also depends on the product in question. In general, the testing phase costs between 10.000 and 30,000 euros.

Box 6 Labelling in Germany

Labelling in Germany

Germany IT Security Label was launched in 2020 in response to an order issued by the Bundestag in March 2017 (BT-Drucksache 18/11808). According to the government, the label scheme allows customers to decide whether they would like to pay in exchange for stronger security and trust instead of mandating the manufacturer to acquire the certification. The IT Security Label also allows to dynamically monitor the security of the product over time. Germany included the Act on the Federal Office for Information Security under the latest IT security.[310]

Whenever a manufacturer wishes to get a label, he submits his product to the BSI – the main security agency in Germany – self-attesting the product compliance with the security requirements provided by the BSI in its Technical Guidelines. Companies have also the freedom to come up with their standards that might be then be proposed to the BSI and eventually included in the Guidelines. The BSI will then check whether the declaration is plausible. Subsequent controls by the BSI will be performed to check the security of the product over time. No ex-ante control is performed by the BSI. The BSI also issues updates for the products when new vulnerabilities are discovered. Every product is marked with a QR code that allows consumers to download patches directly from the producers' website.

An example of a BSI Technical Guideline is the one for Secure Broadband Routers. The Technical Guideline defines mandatory and optional security requirements on routing devices designed for end-users. Among the enlisted requirements there are, for example:

- To prevent attacks on secured connections and on the router itself, all (private) cryptographic keys and secrets MUST NOT be shared by multiple devices in the factory setting and initialized state.
- In factory settings, the router SHOULD restrict access to a defined list of services provided to devices connected to the LAN and WLAN interface by the router.
- In factory settings, the Extended Service Set Identifier (ESSID) SHOULD NOT contain information that consists of or is derived from data or parts of data that depend on the router model itself (e.g., model name).

The costs for companies to get the label is minimal. Companies are only charged for BSI administration costs and have to face some limited internal costs for assessing their declaration.

[310] BSI, Act to Strengthen the Security of Federal Information Technology, 14/08/2009. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=1

Box 7 Labelling in Japan [311]

Labelling in Japan

In Japan, the Connected Consumer Device Security Council (CCDS), an industry association focused on connected consumer devices which are not operated (monitored and controlled) by professionals, launched a voluntary labelling program for IoT devices in October 2019. This program is based on a certification of the products, characterized by a three layers model:

1. Level 1: it includes a common set of requirements as a baseline for IoT devices for all sectors: Automotive on-board devices, Smart Home, ATM, POS, other sectors. It envisages the following mandatory requirements: access control function; a feature to encourage users to change the default passwords; firmware update feature for future security fixes. It started in October 2019.
2. Level 2: it encompasses specific requirements for specific sectors (ex. Banking industry). Started in April 2020.
3. Level 3: it incorporates specific requirements for the protection of users lives and property. Started in April 2020.

Table 57 compares the three labelling models previously described:

Table 57 Labelling models

	Finland	Germany	Japan (level 1)
Scope			
Public-Private Partnership	√	√	√
Voluntary	√	√	√
Mandatory			
IoT Products	√	√	√
IT Products		√	
Subcategory of IoT Products		√	
Type of Conformity Assessment			
Self-declaration	√	√	√
Validation by Public authority	√	√	√
Third-party certification	√		√

Source: OECD (2021b) and Project Teams Interviews with the Finnish and German Government

Table 58Table 58 Label award requirements below compares how the labels are awarded in Finland, Germany and Japan.

[311] For more on this see, Connected Consumer Device Security Council（CCDS）. Available: https://www.ccds.or.jp/english/index.html

Table 58 Label award requirements

	Finland	Germany	Japan (Level 1)
Strong authentication	√	√	√
Remote access control			√
Updatability	√	√	√
Vulnerability disclosure policy	√	√	
Attack surface minimization	√		√
Protection of Personal Data	√		
Encryption	√	√	
Timely updates	√	√	
End of life policy	√	√	

SOURCE: OECD (2021B), AND PROJECT TEAM INTERVIEWS WITH THE FINNISH AND GERMAN GOVERNMENTS

Labelling schemes appear to be a quite "**balanced tool**" to reduce information asymmetries.[312] They have a positive impact on market dynamics without imposing great costs or obligations on producers. Indeed, research suggests that security labels have the potential to impact consumer choice and their willingness to pay for IoT devices.[313] The comparison between the Finnish and the German model shows a significant variation in requirements, product coverage and obligations for producers offering an interesting spectrum of possible applications. Overall labelling schemes for IoT products have the potential to aid consumer decision making and also incentivise manufacturers to ship products that are Secure by Design. However, to be most effective, labels should be used in conjunction with other policy measures, such as ex-ante regulatory requirements, that will be discussed in the context of other policy options.

Codes of conduct

Policymakers can promote code of conducts, voluntary frameworks and guidance to support supply-side stakeholders to enhance the digital security of their products. These frameworks are proposed by the government but quite often are drafted also with the engagement of the industry, civil society and academia and the implementation is voluntary. These frameworks can be very helpful in realigning market incentives. This report presents now some examples of voluntary framework in Europe, Japan and the USA.

[312] OECD (2021), "Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

[313] See Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay . PloS one, 15(1), e0227800.

Code of Conduct in the UK

In the UK, the Department for Digital, Culture, Media and Sport (DCMS) of the UK government in conjunction with the National Cyber Security Centre (NCSC) and with the engagement of industry, consumer associations and academia, published The Code of Practice for consumer IoT in March 2018 as part of the Secure by Design report. This Code of Practice aimed to help all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world.[314] The Code of Practice brings together, in thirteen outcome-focused guidelines, what is widely considered good practice in IoT security, ranging from access control and authentication to vulnerabilities disclosure, data protection, encryption and security updates. Box 8 presents in detail the thirteen components of the UK Code of Practice.

Box 8 UK Code of Practice Components

UK Code of Practice Components

The thirteen components of the Code of Practice are:

1. *No default passwords:* All IoT device passwords shall be unique and not resettable to any universal factory default value.
2. *Implement a vulnerability disclosure policy:* All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy so that security researchers and others can report issues. Disclosed vulnerabilities should be acted on promptly.
3. *Keep software updated:* Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.
4. *Securely store credentials and security-sensitive data:* Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.
5. *Communicate securely:* Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.
6. *Minimise exposed attack surfaces:* All devices and services should operate on the principle of 'least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services

[314] DCMS (2018), Code of Practice for Consumer IoT. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

UK Code of Practice Components

should not be available if they are not used, and code should be minimised to the functionality necessary for the service to operate. The software should run with appropriate privileges, taking account of both security and functionality.

7. *Ensure software integrity:* Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.
8. *Ensure that personal data is protected:* Where devices and/or services process personal data, they shall do so following applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
9. *Make systems resilient to outages:* Resilience should be built into IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and an orderly fashion, rather than in a massive scale reconnect.
10. *Monitor system telemetry data:* If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.
11. *Make it easy for consumers to delete personal data:* Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.
12. *Make installation and maintenance of devices easy:* Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.
13. *Validate input data:* Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Voluntary framework in Japan[315]

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: Society 5.0. In this context, a variety of goods, industries and people will be connected, and this connection will create new value-added while facing new risks such as spreading attack points and increasing impact on physical space. Furthermore, industries will face a shift in supply chains from the conventional stereotypical, linear mode to a more flexible, dynamic one.

[315] This section benefited from an Interview with representatives of the METI on the 4th of November 2020

To meet the cybersecurity challenges 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. [316] 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.

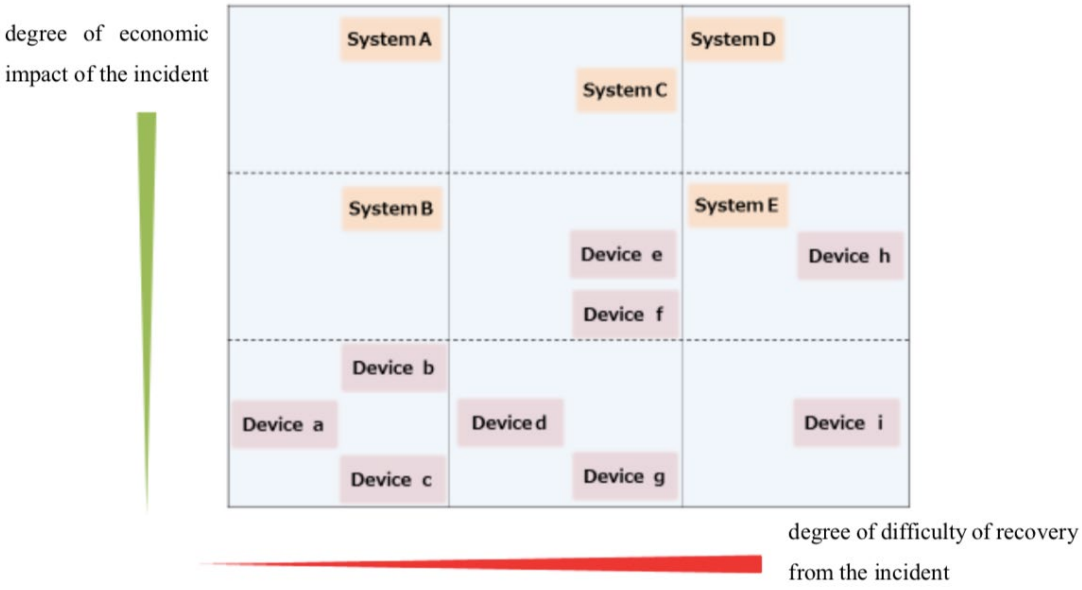
Introducing a unique framework for IoT security is particularly challenging given the great differences among IoT devices and systems. As such, METI introduced a method for classifying IoT devices and systems based on their risk profiles. Particularly, IoT devices and systems are classified alongside two axes and based on the resulting profiles, the systems are linked to different mitigation measures:

- On one axis, IoT devices and systems are categorised based on the degree of **difficulty of recovery from the incidents:** this can take the form of limited damage they could inflict to humans (recovery is easy), serious damage (recovery is not easy), and severe damage (recovery is difficult).
- On the other axis, IoT systems are categorised based on the **perspective of economic impact from the incident,** in the form of limited economic impact (losses), serious economic impact (serious losses) and catastrophic impact (bankruptcy).

As shown in Figure 35, using these two axes, it is possible to map the devices and systems connecting physical space and cyberspace based on their risk profiles. Specifically, METI has identified nine risk categories organizing the risks from the perspective of the difficulty of recovery, in the form of limited damage, serious damage, and severe damage on the first axis, and from the perspective of the economic impact in the form of limited economic impact, serious economic impact, and catastrophic economic impact on the second axis. Based on this categorisation, the appropriate measures for each risk profile can then be envisaged. Consistently, stronger measures will be adopted in case of adoption of devices categorised in the top right of the matrix, while minor measures for those categorised in the bottom left of the matrix. While this categorisation helps define measures to regulate the adoption of the different IoT products and services, it should be noticed that devices categorised under the same risk profile might yet differ greatly depending on their purpose, including what kinds of systems they will be used with, what kind of role they will have in the systems, the skills possessed by the people who will use them, etc.

[316] See METI (2019), Cyber/Physical Security Framework (CPSF) Formulated. Available at: https://www.meti.go.jp/english/press/2019/0418_001.html

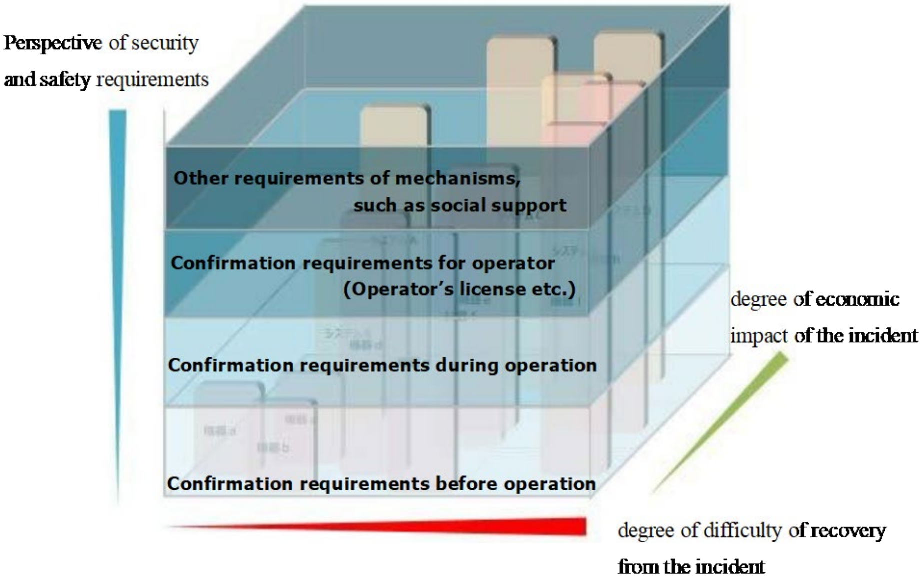
Figure 35 Categorisation of devices and systems connecting physical space and cyberspace



SOURCE: MINISTRY OF ECONOMY (2020) TRADE AND INDUSTRY, IOT SECURITY SAFETY FRAMEWORK SECURING THE TRUSTWORTHINESS OF MUTUAL CONNECTIONS BETWEEN CYBERSPACE AND PHYSICAL SPACE

Starting from this categorisation, it is possible now, using a third axis to envisage different perspectives of desired securityand safety requirements, i.e., different mitigation measures (Figure 36).

Figure 36 Image of the perspectives of the desired security and safety requirements based on the category


Perspective of security and safety requirements
Other requirements of mechanisms, such as social support
Confirmation requirements for operator (Operator's license etc.)
Confirmation requirements during operation
Confirmation requirements before operation
degree of economic impact of the incident
degree of difficulty of recovery from the incident

SOURCE: MINISTRY OF ECONOMY (2020) TRADE AND INDUSTRY, IOT SECURITY SAFETY FRAMEWORK SECURING THE TRUSTWORTHINESS OF MUTUAL CONNECTIONS BETWEEN CYBERSPACE AND PHYSICAL SPACE

The first perspective covers the confirmation requirements before operation - manufacturing phase - and includes self-declaration or certification by a third-party. The second perspective – confirmation requirements during operations – "requires inspecting the devices and systems after the commencement of operations, taking into consideration their life cycle and service period."[317] These measures include voluntary inspections and inspections by third parties. The third perspective regards the confirmation requirements for operators. This is the case in which incidents occurs due to misuse or erroneous operation by people in charge of the devices and systems. In this case, mitigation measures include the review of the operator's license. The last layer of requirements includes capabilities of users, hence, some form of societal support in guaranteeing security such as making enrolment in insurance mandatory in advance.

Hence, the framework is a tool to understand what kind of measures need to be introduced.

As far as the implementation of the framework is concerned, and particularly whether METI is considering shifting form a voluntary based adoption to horizontal legislation, it should be noticed that:

- METI believes that the framework is not the best system to mandate horizontal requirements. The aim of the framework is rather to understand the risk profiles and understand how to deal with these risks. Before being able to mandate requirements, there is a need to have a comprehensive framework that guides companies in understanding the risks.
- Furthermore, METI underlines that IoT is a very new phenomenon that is constantly changing and evolving. As such, having fixed requirements might not produce the desired effect, since the regulation could easily and very soon become outdated. Besides, fixed requirements would not help to achieve better security, and would represent only an additional cost for companies.
- Conversely, METI is trying to promote among companies an attitude of non-stop innovating actions to manage new risks
- Japan has supported this position also internationally, for example by stating that it will not support the Internet Society statement on IoT security if it will introduce policy level requirements.
- There are however some sectors in which regulations could be introduced, for instance, the medical devices. In the case of medical equipment, the regulation requires permission from the government to allow manufacturers to update software, i.e., they cannot do it independently.

Voluntary frameworks in the USA

In the USA, the **National Institute of Standards and Technology** (NIST) in 2018 has designed a **voluntary framework** to support organisation in managing cybersecurity risks. The core of this framework is organised into five functions: Identify, Protect, Detect, Respond, and Recover. These functions should help organisations in managing cybersecurity, by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The focus of the framework is on organisations.[318] As far as products are concerned, in 2019, (NIST) has established the **Cybersecurity for IoT Program** to support the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed.[319] Furthermore, as part of these activities, in May 2020 issued a report

[317] METI (2020), IoT Security Framework Securing the Trustworthiness of Mutual Connections between Cyberspace and Physical Space (Draft). Available at: https://www.meti.go.jp/english/press/2020/pdf/0331_003a.pdf

[318] NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[319] NIST (2020) NIST Cybersecurity for IoT Program. Available at: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

-IoT Device Cybersecurity Capability Core Baseline for manufacturers, also known as NISTIR 8259A. This publication defines an Internet of Things (IoT) device cybersecurity capability core baseline, which is a set of device capabilities generally needed to support common cybersecurity controls that protect an organisation's devices as well as device data, systems, and ecosystems. The purpose of this publication is to provide organisations with a starting point to use in identifying the device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire.[320] Box 9 presents the Cybersecurity Capability Core baseline

Box 9 NIST IoT Device Cybersecurity Capability Core Baseline

NIST IoT Device Cybersecurity Capability Core Baseline

1. *Device Identification*: The IoT device can be uniquely identified logically and physically.
2. *Device Configuration*: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.
3. *Data Protection*: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
4. *Logical Access to Interfaces*: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
5. *Software Update*: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.
6. *Cybersecurity State Awareness*: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

SOURCE: NIST (2020), HTTPS://DOI.ORG/10.6028/NIST.IR.8259A

In this context, it could also be helpful mention the "**Software bill of Material" (SBOM**) initiative promoted by the **National Telecommunications and Information Agency (NTIA)**. It is not a framework nor a voluntary measure but a public-private partnership aiming at increasing the supply chain transparency and reduce cybersecurity risks. Modern software systems involve increasingly complex and dynamic supply chains. Lack of systemic visibility into the composition and functionality of these supply chains contributes substantially to cybersecurity risk. In our increasingly interconnected world, risk and cost impact not only individuals and organisations but also collective goods like public safety and national security.[321] Box 10 below explains in detail the initiative.

[320] NIST (2020). NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline. Available at: https://doi.org/10.6028/NIST.IR.8259A

[321] See NTIA (2019), Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM). Available at: https://www.ntia.doc.gov/files/ntia/publications/framingsbom_20191112.pdf

Box 10 Software Bill of Materials (SBOM)

Software Bill of Materials (SBOM)

Software is a primary component of ICT products and systems, and with the latest development of, among others, IoT or industrial control, embedded systems are even more dependent on complex software. Software vulnerabilities are nonetheless increasingly frequent, due not only to human errors but also to the lack of transparency in the software supply chain, which makes the supply-chain a growingly easy target for cyber-attacks. Software dependency on third party components (libraries, executables, source codes) which are not well identified or recorded indeed makes it harder for users to patch the software and to understand if it contains malicious components.

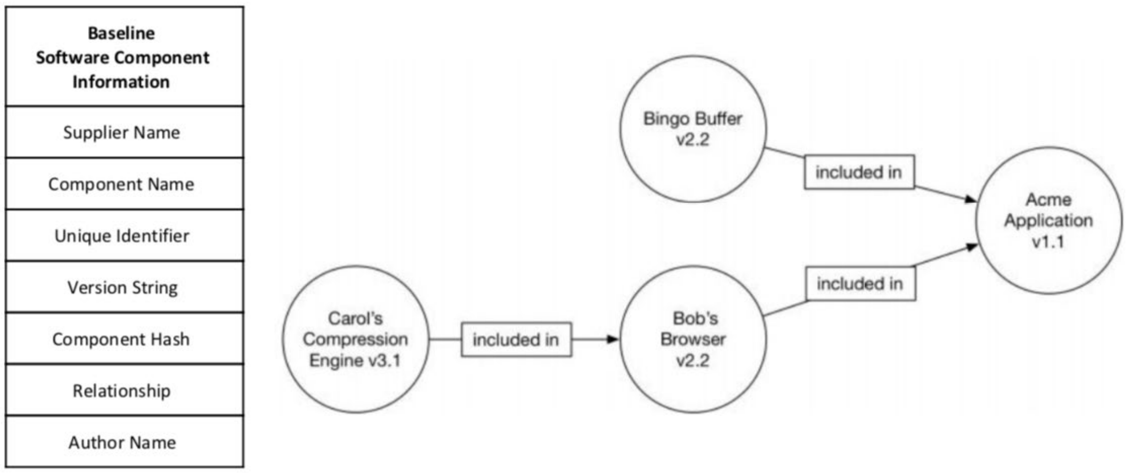
Greater transparency on the software components and supply chain would allow earlier identification (and mitigation) of potentially vulnerable systems, support informed purchasing decisions and incentivize secure software development practices. The idea of a *list of ingredients* is not particularly new, but current trends in security make transparency essential. In particular, it has been mentioned the “need to rapidly respond to known or potential exploits targeting software components such as the Urgent/11 or Ripple20 vulnerabilities.” Moreover “IoT, industrial control, medical devices, and embedded systems are particularly important in safety-critical applications and are ever-more dependent on complex software. Introducing SBOMs into these technologies today will help us better respond to risks tomorrow.” Furthermore, with SBOM data, it would be possible to prioritize open-source security and understand, for example, which open-source software or third-party components can give a malicious actor the greatest advantage.

To foster software transparency, the National Telecommunication and Information Administration (NTAI) has developed a cross-sector, multi-stakeholder process on Software Component Transparency which envisaged and encouraged the adoption of the Software Bill of Material (SBOM). The Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of the various components used in building software. Hence, the components, the information about these components, and the relations among them are listed and identified in SBOM. Other than defining what SBOM is, the NTAI process also documented the security and economic benefits of using SBOM as well as the existing standards that can be used to automatically convey SBOM data (such as SPDX, SWID and CycloneDX).

To uniquely and unambiguously identify components and their relationships, some combination of the Baseline Software Component Information – Supplier Name, Component Name, Unique Identifier, Version String, Component Hash, Relationship, Author Name – is required. It is possible that not every SBOM entry will require or be able to provide each of the baseline attributes. Certain attributes (e.g., Component Hash) provide greater uniqueness or unambiguity.

Baseline SBOM

Software Bill of Materials (SBOM)



Baseline Software Component Information

Supplier Name

Component Name

Unique Identifier

Version String

Component Hash

Relationship

Author Name

Figure 1: The baseline SBOM includes components in their assembled relationship. Each component has enough information to "uniquely and unambiguously identify" it (left), and the relationship of what upstream or child components are "included in" downstream or parent components (right).[2]

SOURCE : HTTPS://WWW.NTIA.GOV/FILES/NTIA/PUBLICATIONS/SBOM_OVERVIEW_20200818.PDF

A new SBOM should be created for every new release of a component. Changes to components require corresponding changes to SBOMs, often noted as updates, upgrades, releases, and patches. Different stakeholders (those who produce, choose, and operate the software) will use SBOMs in complementary yet distinct ways.

Several notable applications of the SBOM have been highlighted:[322]

1. **Vulnerability Management**: Vulnerability management is one of the more prominent applications because of the difficulties in determining whether a vulnerable subcomponent is used and if the vulnerability transitively makes the downstream component vulnerable or exploitable. SBOM data helps suppliers, users, etc. to more accurately define the risk posed by vulnerable components otherwise hidden behind supply chain relationships. Additional information needed: sources of vulnerability information such as CVE and the NVD.

2. **Intellectual Property**: Several intellectual property applications could be improved with better inventory data such as the management of software licensing (including constraints on use or redistribution) for included components and tracking entitlement. Additional information needed: associations of different licenses and types of licenses to components, and a way to evaluate the net effect of different components with different licenses combined into an assembled good. Both SPDX and SWID were designed to carry license information.

3. **High Assurance**: SBOM helps in guaranteeing high assurance of the source and integrity of components requiring information about suppliers, how components are built, the chain of custody as components move

[322] NTIA (2019) Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM). Available at: https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

Software Bill of Materials (SBOM)

through the supply chain, and how any modifications are made. Additional information needed: information about the pedigree and provenance of components, such as how they were built.

In addition to the specific additional applications identified above, other sets of information could be useful, including end-of-life dates, indication on what technologies a component supports, information about groups of components (around technologies or other concepts) - for example, “component X implements DNS” allowing users to identify all DNS-relevant components.

Challenges for the development of voluntary frameworks[323]

The development of a voluntary framework should take into account two critical issues: **fragmentation** and **lack of uptake.** First, the government should avoid producing new frameworks when industry or international standards already exist. Indeed, unnecessary frameworks could generate market confusion and fragmentation. The government should use frameworks to close gaps in the practices already available for the stakeholders.

Second, if the framework generates a limited uptake, additional measures such as mandatory requirements are probably needed.

Finally, it is important to stress that voluntary frameworks are tools used to address the issue on the supply side of the value chain. To involve also the demand-side of the value chain, a joint combination with labelling systems is recommended.

Government procurement Policies

Putting in place a framework for public procurement entails establishing purchasing priorities and decision. By procuring and using products that have sufficient security and integrity, buyers can consistently reduce the risks they are exposed to as well as incentivize suppliers to develop and provide more secure products, given that through their purchasing decision they can influence the market development

In this context, governments have a great role to play in influencing market purchasing security standards. Indeed, governments can require ICT suppliers operating within their jurisdiction to comply with certain security, data protection, privacy, or related requirements or commitments. Buyers need to be sure that the specific requirement imposed by the governments are met by suppliers, as such fostering assurance and increasing the overall level of security within a system. This holds, even more, when governments act as buyers of ICT products themselves.

Furthermore, procurement policies could mention the specific cyber and supply chain security requirements that the vendors should satisfy to be qualified as “original manufacturers or authorized resellers”.

[323] This section draws from OECD (2021), "Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

There are two ways in which suppliers can demonstrate assurance to buyers:[324]

- **Self-attestation:** It entails supplier provision of evidence that it is adhering to security commitments that could be embedded in standards, best practices or other positions about which it has made public or private statements. Self-attestation is especially relevant in the circumstances in which a third-party attestation of compliance is not available due, for example, to time constraints. It allows buyers to gain greater insight into process and practices put in place by suppliers as well as into the products and services themselves, thus fostering an ecosystem of trust among the parties. As such, self-attestation is also relevant when ICT buyers require a more granular understanding of how a supplier develops its products or services. For example, "buyers making long-term procurement commitments may require elevated confidence in a supplier's ability to comply with relevant laws and regulations or contract commitments."[325]
- **External attestation:** Audits and certification against international standards are forms of external attestation. Particularly, this process of demonstrating assurance must involve a third party other than the suppliers able to evaluate and eventually attest the suppliers' adherence to given security commitment. In this context, audits can be performed against an international standard such as ISO 27001, a leading information security standard, or the ISO/IEC 20243. The latter in particular address product integrity and supply chain security best practices to reduce the risks associated with taint and counterfeit. It applies to process used throughout the ICT products' lifecycle – from design to disposal, including software, hardware and supply chain – and includes requirements for suppliers. As such, it seems to be particularly fit for purpose. The benefits of relying on third-party attestation, other than providing assurance, relates to the buyer's time management. Indeed, it saves buyers the time and resources they would need to spend asking questions and validating the answers from each of their suppliers.[326]

Public procurement policies for ICT products in Scotland

Scotland is an example of the adoption of a framework for the public procurement of ICT products encompassing security aspects. To embed cybersecurity into the public sector supply chain and protect against cyber-attacks the country developed the **Scottish Cyber Assessment Service and the Supplier Cyber Security Guidance Note.** The former is an online tool for public procurement requiring suppliers to complete a questionnaire detailing their current level of cybersecurity (aligned with guidance from the National Cyber Security Centre). The risk level of a contract is assessed based on the level of system access and information sharing with the suppliers. For high-risk application, the control is aligned with the NCSC NIS Technical Guidance and with ISO27001.[327]

National government procurement policy for ICT products in the Netherlands[328]

The Dutch government believes that public procurement policy can boost the demand for secure digital products. Such a policy not only improves the level of cybersecurity of ICT products that the government purchases for internal

[324] EastWest Institute (2016), Purchasing Secure ICT Products and Services: A Buyers Guide. Available at: https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf

[325] *Ibid.* p. 18

[326] *Ibid.* p. 19

[327] Scottish Government, Public Procurement. Available at: https://blogs.gov.scot/public-procurement/2020/02/18/improving-procurement-cyber-security/

[328] This section benefited from an interview with the Dutch Government on the 9th of December.

use, but also stimulates the whole cybersecurity market. Producers can indeed get a return for their investments by publicizing that the government has purchased their products.

To control public procurement, a tool has been developed that supports government organisations when purchasing ICT products and services. The tool has been online since March and it is available as a prototype. An expert group with representatives from the Central government, provinces and municipalities have formulated procurement requirements for eleven purchasing segments, such as cloud services and server platforms. The tool is now being tested in pilots in various government organisations. At the end of the piloting phase, (approximately two years) requirements for public procurement will be mandated.

Public Procurement policies for ICT products in Germany [329]

The IT Security Label system developed in Germany is useful also in the context of public procurement in case consumer products are being purchased by the public sector. However, it should be noted that Germany distinguishes the public sector from the administration. For example, stricter requirements are established for critical infrastructures (hospitals, energy providers, etc.) and even more, requirements are envisaged by the BSI for the adoption of IT products by the Federal Government. As such, the security level that is required for public procurement is not comparable to the one acquired through the labelling system.

Public procurement policies for ICT products in the USA

The U.S. Department of Defence (DoD) released the first version of the Cybersecurity Maturity Model Certification (CMMC) back on January 31, 2020.[330] Before then, the NIST 800-171 was used to allow companies contracting with the DoD to show that they were protecting Controlled Unclassified Information (CUI). This process was based on a self-certification that companies were meeting the NIST 800-171 requirements.

Instead, the CMMC now requires a third-party assessment of the contractor's compliance with the CMMC. The CMMC is characterized by 5 maturity levels: Basic cyber hygiene, Intermediate Cyber Hygiene, Good Cyber Hygiene, Proactive and Advanced. Each level represents some ad hoc functions that different contractors will have to meet. Each level increases the requirements, so a contractor at level 2 would have to meet level 1 & 2 requirements, while a company at level five would have to meet all the requirements for level 1-5. Each level establishes a different level of cybersecurity maturity.

Following the recent SolarWinds attack in the USA, there have been further calls for a stronger intervention by the US Government to improve the security of supply chain through better government software procurement and for setting minimum safety and security standards for all software sold in the United States. [331] Therefore, on the 12th of May 2021, President Biden, has issued an Executive Order designed to improve supply chain security, incident detection and response and overall resilience to threats.[332]

[329] This section benefited from an interview with the German Government on the 8th of December.

[330] Steven Tipton (2020), Cybersecurity Maturity Model Certification (CMMC) and Why You Should Care. Available at: https://www.tripwire.com/state-of-security/regulatory-compliance/cybersecurity-maturity-model-certification-cmmc/

[331] Schneier B. (2021), "The SolarWinds hack is stunning. Here's what should be done", CNN, January

[332] Muncaster P. (2021), "Biden Executive Order Mandates Zero Trust & Strong Encryption", Infosecurity Magazine, 21 May.

Using Public procurement to guarantee cybersecurity of ICT products implies a low probability of market distortion but to be more effective should be used jointly with other measures.

Awareness campaigns

Increasing awareness on digital security and in particular on the security of ICT products through media campaign and ad hoc training in schools and universities is another tool that policymakers can use to reduce information asymmetries and market failures in the ICT product markets. In the EU the European Commission is devoting each year a full month to cybersecurity awareness campaigns. The European Cybersecurity Month (ECSM) under the coordination of ENISA is one of the mechanisms by which cyber hygiene and awareness are promoted to citizens and businesses of Europe.

The growing pace of security breaches, the multiple facets of information security requirements, and potential growth and trends in the incident response market put an ever-increasing burden on training qualified and capable personnel to provide commensurate response services to fulfil these needs. As safety and security become intertwined "cultures and working practices will change. Safety engineers will have to learn adversarial thinking while security engineers will have to think more about usability and maintainability." This will require to redesign the university's curricula especially for software engineers where security and safety would need to be envisaged as two aspects of the same mission: designing systems that mitigate harm, whether caused by adversaries or not."[333]

Awareness campaign in the Netherlands

In the Netherlands, the government promotes behavioural studies/campaigns aimed at fostering ICT security. Designers can/should be made more aware of the importance of applying security by design; purchasers can/should be alerted to reliable/unreliable products, and users can/should be encouraged to maintain their products' security. Awareness campaigns are promoted based on the acknowledgement that consumers are not able to address alone security problems. As such, it is the responsibility of the government to foster their responsible behaviours. In this context, for example, the Dutch government is promoting the third edition of the "**Do your updates"** campaign to actively urge people to make sure their devices are updated and safe against cybercriminals. The campaign is promoted through online channels, radio commercials and music services. From the evaluation of the first two rounds of the campaign, it has been noticed that the creative design of the campaign works well for conveying the message, but that it is necessary to repeat the campaign to bring about behavioural changes. Together with the Ministry of Justice, a campaign against phishing is also being promoted. Furthermore, the Dutch government is also promoting the development of safety and security frameworks in the university's curricula. In particular, is working towards implementing secure software development in university curricula.

[333] Leverett E., Clayton R. and Anderson R, (2017), Standardization and Certification of the Internet of Things, mimeo, p. 22.

Awareness campaign in Germany

The German government is planning an awareness campaign on IoT security especially for consumers. In particular, they are thinking to use the Cybersecurity awareness month in the EU for this purpose.

Overall, promoting awareness campaigns does not bear the risk of distorting the market, but at the same time cannot be used as a substitute for other measures previously mentioned. In other words, it should be used but as an accompanying measure.

Evaluation of the policy option Voluntary measures

The previous sections have offered a detailed analysis of the policy measures that could characterize the policy option: **Voluntary measures**. Table 59 presents a synthetic view of the characteristics of this policy option and Table 60 a comparison of the plus and minus of the policy measures.

Table 59 Voluntary Policy Measures Description

Policy measures	Description	Examples
Voluntary Certification as defined in the Cybersecurity Act	Conformity assessment for evaluating whether specified requirements relating to an ICT product, services or process have been fulfilled	- IoT Labelling in Finland - IT Security Label in Germany - EU-CC, Cloud Services schemes, - Certification scheme for IoT*
Code of Conducts	Policymakers can promote codes of conducts, voluntary frameworks and guidance to support supply-side stakeholders to enhance the digital security of their products	- UK The code of Practice for Consumer IoT - IoT Security Safety Framework in Japan - NIST Framework of 2018 and the IoT Device Cybersecurity Capability Core baseline in 2020
Government procurement policy	Governments can require ICT suppliers operating within their jurisdiction to comply with certain security, data protection, privacy, or related requirements	- Scottish Cyber Assessment Service and the Supplier Cybersecurity Guidance note - Cybersecurity Maturity Model Certification (CMMC) in the USA
Awareness-raising campaigns	Increasing awareness on the security of ICT products through media campaign and ad hoc training in schools and universities	- European Commission Cybersecurity Month (ECSM) - *Do your update* and against fishing campaigns in the Netherlands - The German government is planning an IoT security campaign for consumers
Commission Recommendations		
Industry-led initiatives		

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Table 60 Voluntary Policy Measures Comparison

Policy measures	Plus	Minus
Voluntary Certification as defined in the Cybersecurity Act	Increase products security and consumers' trust Labelling: Reduce information asymmetries	Self-assessment presents high risks of non-compliance related to a low degree of market surveillance. Third-party certification presents risks in terms of: - Costs - Issue of scalability for IoT devices - Not valuable for mainstream users - Potential "insecurity by compliance"

Codes of Conduct	Realign incentives	- Too focused on the supply-side - Fragmentation - Lack of uptake
Government procurement policy	Low probability of market distortion	To be more effective should be used jointly with other measures
Awareness-raising campaigns	Increase consumers awareness	- Cannot be used as a substitute for other policy measures but as accompanying other policy measures
Commission Recommendations		
Industry led-initiatives		

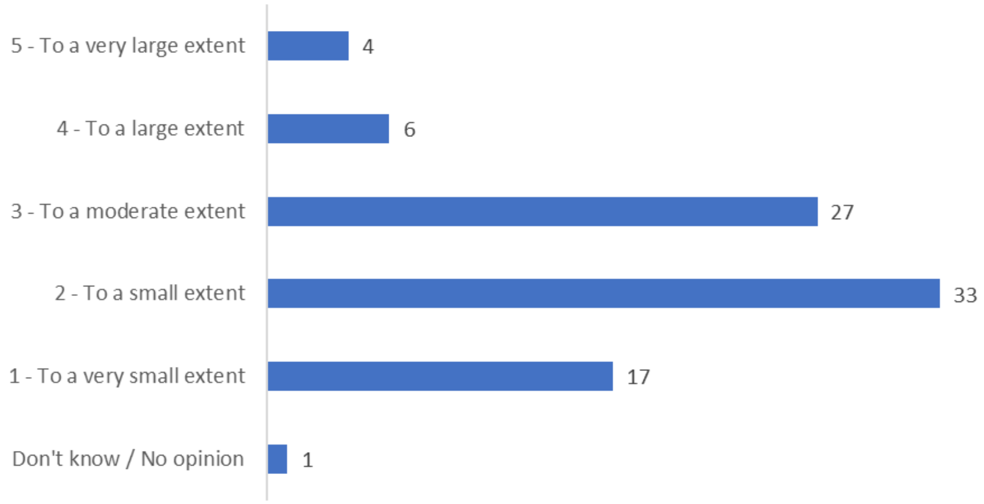
Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

During the third workshop, held on 4 February with 126 participants and focused on the policy options, participants have been asked to express their preference on the different policy measures envisaged under Policy Option 1: Voluntary measures. The results show a relative preference for the Policy measure Voluntary certification as defined in the Cybersecurity Act (41 out of 126 respondents, or 33%) and Industry-led initiatives (25 out of 126, or 20%).

Participants to the workshop stressed that the costs of voluntary measures could outweigh the benefits insofar as companies willing to voluntary implement the measures will have to face the competitions of companies not willing to implement them. This also relates to the market failure (market for lemons) that characterizes the cybersecurity market because users will be hardly willing to pay the extra costs stemming from the implementation of the measures.

Respondents to the targeted consultations most frequently rated voluntary measures as addressing the need for cybersecure ICT products to a small or very small extent: 33 of the 88 respondents (37%) rated this policy option as addressing the issue to a small extent while 17 (19%) thought it did so to a very small extent. 27 respondents (31% of the total sample) rated this policy option as addressing the need for cybersecure ICT products to a moderate extent.

Figure 37 Extent to which adoption of voluntary measures address the cybersecurity needs of ICT Products



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

Respondents were also asked which measures under policy option 1 would be the most relevant to address the need for cybersecure ICT products**. Government procurement policies** were judged as the most significantly relevant (by 39% of the respondents) compared to all others. Just over a third of the respondents (34%) judged that those voluntary certifications as defined under the CSA would be the most significantly relevant. Notably, a respondent on behalf of the ICT industry indicated that while all the above measures were relevant, some additional ones could be considered such as self-assessment, training of professional and end-users, and exchange of best practices.

Similarly, there was consensus among the NCAs that voluntary measures would be too resource constraining to be taken up by most ICT companies, especially the smaller ones. As such, voluntary measures would not be sufficiently conducive to more secure ICT products overall. This idea was confirmed by respondents on behalf of the ICT industry who argued that voluntary measures would favour ICT companies who are large enough to implement processes on security and which can communicate effectively.

Overall, voluntary approaches to ICT products security could, as mentioned above, foster innovation and competition compared with stricter regulatory measures. The adoption of voluntary measures might thus theoretically be the preferable course of action. Such an option would not have negative impact on innovation and would not risk unduly raising firms' costs. It is the self-disciplinary force of competition that is better placed to drive companies to adopt state of the art measures, in order to overtake or at least meet competition. However, experience shows that such positive trust in competition may work well if customers are sophisticated and capable of exercising buyers' power, driving competing business to a race for the top (see the case of cloud based B2B services).This might not be the case when buyers/end users are not capable of exercising any real countervailing/disciplining force (such as would be the case for consumers), or when the market is characterized by strong market failures and strong power unbalances among market players. While security conscientious vendors will try to design the best products for their customers, the lack of buyers' competence in comparing the security attributes of different ICT products can lead to an unfair competition where the price is favoured to the detriment of security.

Hence, voluntary measures might prove ineffective, as the incentive to cut costs might prevail over the perceived advantage of offering more secure ICT products.[334]

5.2.3 Analysis and specification of the Policy Option 2: Horizontal Legislation

Introduction

When presenting the policy option "Voluntary measures", it has been mentioned that many governments have favoured voluntary approaches to ICT products security afraid that regulatory intervention could stifle innovation and competition. The fast-changing technological landscape of these markets played also a role, suggesting avoiding ex-ante regulation due to the quick obsolescence of the measures implemented. However, the increasing volume and scale of the threats and their multifaced nature combined with the numerous asymmetries and market failures that characterize ICT products markets, have recently suggested a more proactive role by the governments.

[334] Contributed by L. Montagnani, member of the Advisory Board of the Project.

In the EU there have been quite a few calls from EU Institutions for mandatory rules to increase the digital security of ICT products. On the 2nd of December 2020, the Council of the European Union in its Conclusions on the cybersecurity of connected devices underlines "the importance of assessing the **need for horizontal legislation**, also specifying the necessary conditions for the placement on the market, in the long-term to address all relevant aspects of cybersecurity of connected devices, such as availability, integrity and confidentiality."[335]

On the 16th of December 2020 the European Commission in its Communications on "the EU's Cybersecurity Strategy for the Digital Decade, in the section on "An Internet of Secure Things", mentioned that the Commission "will consider a comprehensive approach, **including possible new horizontal rules** to improve the cybersecurity of all connected products and associated services placed on the Internal Market."[336]

In the interviews conducted by the Project Team with the governments of Finland, Germany and the Netherlands on their initiative for the cybersecurity for ICT products, the prevailing message was that their current initiatives, although voluntary at the moment, were to some extent instrumental to the definition of some type of ex-ante common rules for cybersecurity for connected devices at the European level.

The Finnish government, for instance, does not oppose the idea of setting binding regulations for higher-level requirements as long as immediate actions tackling basic security features are addressed. However, an incremental approach would be preferred because of the limited understanding of information security and since the requirements should be set in such a way that they could be easily tested.

The challenge faced by Germany was that the access to the EU market could only be regulated on the basis of European harmonized rules. As such, there was no possibility for issuing national mandatory minimum requirements for consumer IoT products. Because of this, the Ministry of the Interior, Building and Community is developing a voluntary labelling system, where the manufacturer would be the main responsible for the security of the product, while the BSI would be responsible for the consumers' protection. Notably, if Germany would have had the possibility to directly issue mandatory security requirements, it would have preferred this option. Therefore, while the IT Security Label is being developed, their long-term objective would be to establish mandatory requirements for IT products' security. In this respect, Germany would like the IT Security Label to serve as a blueprint for an EU harmonized approach. Principles from the IT Security Label could be extracted to establish an EU horizontal regulation; however, the scope should be extended to applications other than lower-risk consumer products. Germany supports such a broadening of the IT Security Label scope.

Finally, the Dutch government supports the adoption of binding regulations for ICT products and services. However, it does not envisage to issue horizontal regulations at the national level because the country advocates for a harmonized approach at the EU level. European-level legislation would indeed help the level playing field. This aspect is particularly relevant for the Netherlands whose companies would otherwise suffer from foreign competition.

But probably the most relevant case that shows support for embracing horizontal legislation is the UK case. As mentioned in the previous section, the UK government started suggesting a voluntary approach through the publication in 2018 of a Code of Conduct for IoT Consumer products. Recently, DCMS moved toward a minimum set of requirements mandatory by law (Consultation in July 2020). The UK moved from a voluntary approach to

[335] Council of the European Union (2020), Council Conclusions on the cybersecurity of connected devices. 2 December, page 4
[336] European Commission (2020), The EU's Cybersecurity Strategy for the Digital Decade", page 9.

more legally binding measures due to growing evidence suggesting that good practices were not being implemented. Indeed, when the UK published the Code, it monitored the adoption of the good practices shared also with ETSI. While the hope was that these good practices would have been enough, by kept monitoring their adoption, the UK realized that a more horizontal approach was needed.

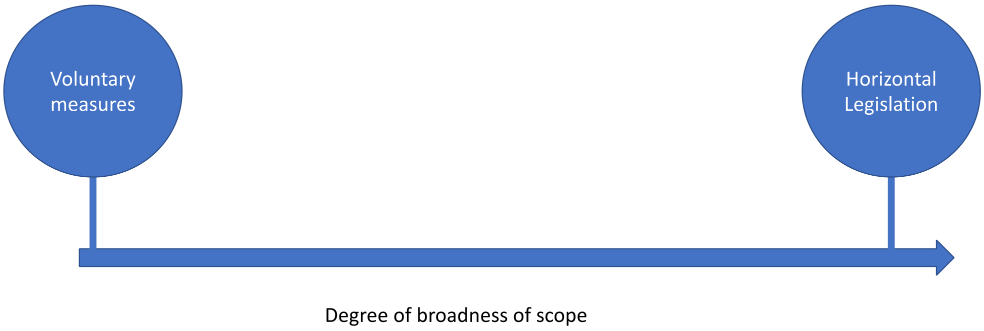
Also, some organisation of the private sector such as Orgalim and some Consumer organisations such as BEUC and ANEC are calling for the implementation of Horizontal legislation on cybersecurity for ICT products.[337]

What is meant by Horizontal Legislation?

For the purpose of this study, the Project Team will define **horizontal legislation as a set of requirements applied to all sectors and categories of products whose producers and vendors shall comply with, before placing the products on the market (*ex-ante*) and also through the entire product lifecycle (*ex-post*).**

Figure 38 below present the "location" of the Horizontal legislation option in the cybersecurity policy option space.

Figure 38 Horizontal legislation option in the cybersecurity policy option space



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Since the horizontal legislation is characterized by a set of requirements applied to all sectors and categories of products it gains the maximum value in terms of degree of broadness of scope.

Policy option specification of a common regulatory approach applicable to all sectors and categories of ICT products

The specification of the policy option" horizontal legislation" entails the definition of a common set of requirements and their application to all sectors and categories of ICT products.

[337] ORGALIM (2020), Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework, Policy Paper, 9 November. BEUC (2019), KEEPING CONSUMER SECURE – How to tackle cybersecurity threats through EU law,

As a starting point, the rules would be framed in the context of the EU NLF. [338] Since the NLF suggests a toolbox of measures for use in product legislation. The Project Team has selected the main policy measures of the NLF that can be applied to cybersecurity for ICT products. In particular, the Project Team has focused on:

- Essential requirements;
- Conformity assessment; and
- Market surveillance.

Essential requirements

The essential requirements are high-level requirements for ICT products and are not technology specific and should in principle be applicable to broad categories of products. Requirements may apply to the product itself (e.g., the product should have certain features) or to processes related to the design, development, delivering or maintaining of the product. The essential requirements are set out in the legislation, and are not the result of the manufacturer risk assessment. Table 38 in Section 4.2 presents the Cybersecurity essential requirements as envisaged by the Project Team.

These requirements are considered essential and therefore should be applied to all categories of products and sectors. No “a la carte menu” is envisaged by the Project Team. Requirements cannot be chosen by the economic operators. To which sectors and products should these requirements be applied? The sectors and products categories have been identified by the work of task 2 and are presented in Table 15. Since this study has an exploratory nature, this table should not be considered exhaustive. For each cell of the matrix, the Project Team also identified the proper risk level which is presented in Table 31. This table shows that in a given sector, the risk profile is not the same for all ICT products categories. For instance, in Smart Home the risk profile for the ICT category “End Devices” is higher than for “Networks”. At the same time, for a given ICT products category the risk profile is not the same across sectors. This is the case of the ICT product category “Security” that has higher risk profile for Finance than for Smart home. This implies that it is not possible to define single risk profiles per ICT product category or per sector. Also, the risk profile of a specific ICT Product may vary between sectors. Therefore, the risk profile should be handled carefully in the definition of the policy options and should be established based on the **product’s intended use** rather than on rigid classifications of the products’ risk profiles.

Conformity Assessment

Conformity assessment procedures/methods define how compliance to requirements is assessed. As shown in Section 4.3, the Project Team has identified a set of applicable conformity assessment methods that apply both ex-ante and ex-post to ensure that the security of the product once placed on the market is also assessed.

Conformity assessment could be carried out by the manufacturer/vendor or a third party depending amongst others on the risk involved and possibly the nature of the product. In this context, a specific role could be by the mandatory or non-mandatory involvement of notified bodies.

[338] European Commission (2016), Commission Notice- The Blue Guide on the Implementation of EU Product Rules, Official Journal of the European Union, 26 July, p.39

Market Surveillance

In the context of Cybersecurity for ICT products, beside the current rules for market surveillance envisaged by the NLF, since it is required to guarantee security through the entire lifecycle of the products it is necessary to extend the post-market surveillance activity to guarantee the security of product during the usage phase and when the products are removed from the market.

In particular, the following initiatives could be promoted:

- Sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors;
- Vulnerability remediation;
- Incident response;
- Product phasing out;
- Production of **Post Market Surveillance (PMS) Plan** and **Post market Reports** (**PMSRs**); and
- Auditing.

Furthermore, attention should also be given to the **proper identification of the authorities** that should take care of the violation of the security requirements since, at the moment, the allocation of responsibilities among authorities is not clear.

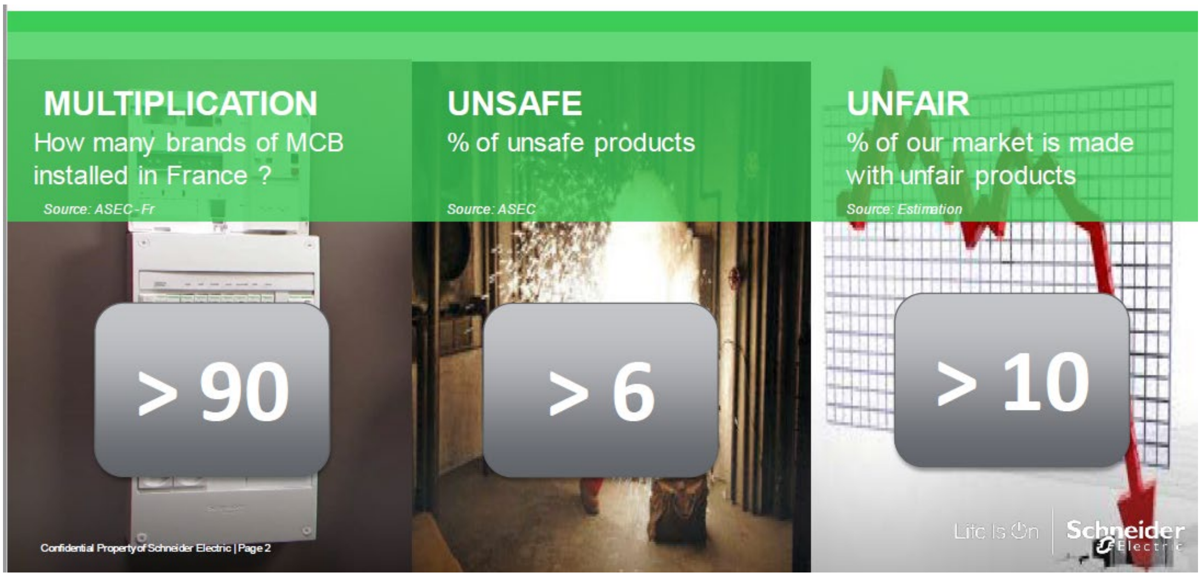
First, adding the digital layer to the activity of the current market surveillance authorities, will require increasing resources and means for the market surveillance authorities to face the new challenges.

Currently, there is a **lack of human and financial resources** devoted to Market Surveillance Authorities, which are already severely impeded in their enforcement abilities. According to various sources, as shown in Figure 8 the amount of insecure and unfair products being placed in the market is quite high and roughly accounts for 6% of hazardous products and 10% of unfair products (both nonconformity and counterfeit products).

As such, it would be challenging to increase the tasks of Market Surveillance Authorities already overburdened and lacking the capacities to carry out their current duties. Market Surveillance Authorities must be allocated with the appropriate **financial and human resources and cybersecurity skills**. The lack of appropriate means for Market Surveillance Authorities to carry out their activities would also have a detrimental effect on fair players compared to rough actors exploiting the lack of proper enforcement.

Horizontal legislation should also ensure competent authorities to act under the same rules and apply the same methods across Europe to ensure coherence and a level playing field within the single market.

Figure 39 Market Surveillance Resources Gap[339]


MULTIPLICATION
How many brands of MCB installed in France ?
Source: ASEC-Fr
> 90
UNSAFE
% of unsafe products
Source: ASEC
> 6
UNFAIR
% of our market is made with unfair products
Source: Estimation
> 10
Confidential Property of Schneider Electric | Page 2
Life Is On
Schneider Electric

SOURCE: SCHNEIDER ELECTRIC (2020)

In terms of identification of the competent Surveillance Authority, the following two options could be put forward:

- **One central authority (one-stop-shopping) in each Member State:** The current cybersecurity authority would manage the digital layer of all the ICT products. In this context, it would be very important to guarantee the level playing field across Europe, ensuring the same competencies across member states. It is important to guarantee the level playing field across Europe, ensuring the same competencies across member states. As such, one single authority performing market surveillance would be advisable.
- **Sector-specific Surveillance Authorities**: Since it might be challenging to ensure that a single governing agency would have enough expertise to address the security of all product categories, in this case the digital layer would be added to the current market surveillance authorities. Besides, it would be important to ensure harmonization and information sharing among the sectoral authorities.

Given the complexities of the matter, the decision regarding which authority would be best fitted for performing cybersecurity market surveillance might be left to the Member States.

Summing up, the Horizontal Legislation policy option entails a set of requirements applied to all sectors and categories of products whose producers and vendors shall comply with, before placing the products on the market and also through the entire product lifecycle. The policy measures that characterize this option are: a set of essential requirements, conformity assessment rules and market surveillance policies.

Table 61 summarises the characteristics of the Horizontal legislation policy option.

[339] The source of the first figure is a CONSUEL studies on behalf of ASEC carried out every 2 years since 2014. The source of the second figure is an analysis carried out by ASEC since 2008 mainly on Miniature Circuit Breakers and Residual Current Circuit Breakers. The source of the third figure is an estimation based on Schneider Electric's field experience and commonly accepted by other stakeholders. In certain geographical areas outside Europe, such as Africa, this percentage can rise up to 80%. For more on these see: http://www.securelectrique.com/ and http://mssi-electrical.org/en

Table 61 Policy Option Horizontal Legislation

		Policy Option 2 – Horizontal Legislation
		Implementation of a common regulatory approach applicable to all categories and risk profiles of ICT products
Policy Measures		
Essential Requirements		Definition of essential requirements. applied to all sectors/products
Conformity Assessment	*Mandatory involvement of notified bodies*	√
	Non mandatory involvement of notified bodies	√
Lifecycle	*All*	√
	Some	
Risk Profiles	*All*	√
	Some	
Product/ Sector Categories	*All*	√
	Some	
Market surveillance	Sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors	√
	Vulnerability remediation	√
	Incident response	√
	Production of Post Market Surveillance (PMS) Plan and Post market Reports (PMSRs)	√
	Auditing	√

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Stakeholders' feedback on the Horizontal legislation

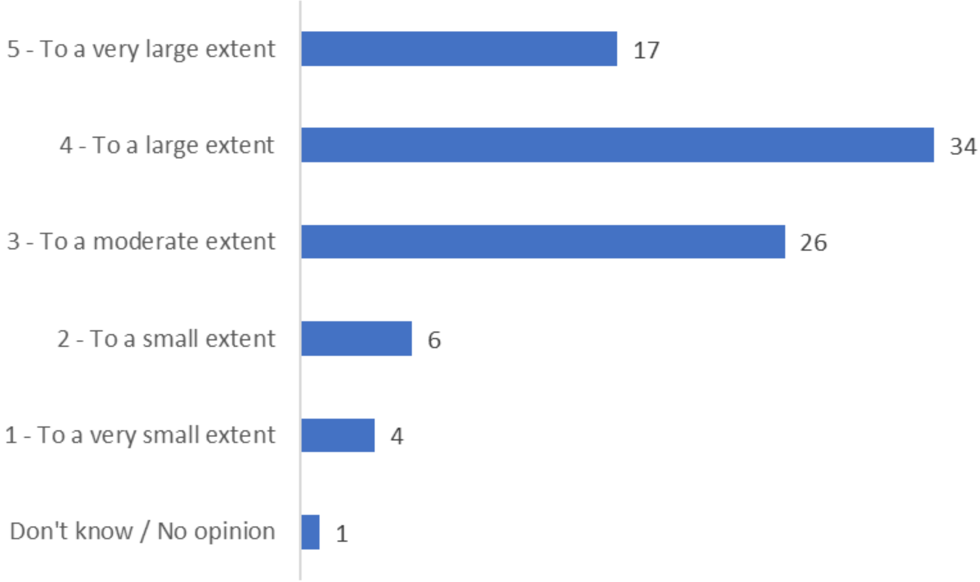
To get a preliminary feedback on the impact of the Horizontal Legislation policy option, the Project Team has conducted 14 interviews with industry representative and consumer organisations.[340] These findings were complemented by the targeted consultation.

The Horizontal legislation policy option was overall most frequently rated as addressing the need for cybersecure ICT products to a large or a very large extent by respondents to the targeted consultation. 34 of the 88 respondents

[340] The interviews have been conducted between the 13th and the 29th of January and have involved the following entities: ANEC, Atos, BEUC, Business Software Alliance, Digital Europe, ETNO, Huawei, NXP, Orgalim, Microsoft, Schneider Electric, Siemens, TUV and ZVEI.

(37%) rated this policy option as addressing the issue to a large extent while 17 (19%) thought it did so to a very large extent.

Figure 40 Extent to which the establishment of a horizontal legislation for ICT products and services would address the need of cybersecurity of ICT products



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

The great majority of stakeholders consulted through individual interviews also positively welcomed the idea of establishing horizontal legislation for addressing the need for cybersecurity for ICT products. Horizontal legislation would help to mitigate the risk of different requirements being placed on products that fall under several Directives simultaneously. Hence, it would reduce the risk of double jeopardy and regulatory uncertainty. Horizontal legislation might also be a more appropriate tool for improving the level of cybersecurity in the EU than the application of other legislation not originally intended to do so - such as ex-ante instruments through the Radio Equipment Directive. The RED aligned the previous directive (1999/5/EC) with the NLF and defines the regulatory framework for the placement of radio equipment on the market. In this context, for example, a horizontal approach would more coherently and more broadly address the need for cybersecurity for ICT products compared to product-specific legislative instruments.

Similarly, ICT industry players participating in the targeted consultation suggested that a horizontal approach will avoid the legal uncertainty caused by the currently patchwork of security requirements in several overlapping pieces of legislation. Furthermore, a horizontal approach could provide better support for other proposed legislative changes such as the NIS2.

In this context, while welcoming a horizontal approach to ICT cybersecurity, most interviewed stakeholders underlined that the legislation should be carefully scoped to avoid the risk of introducing any overlap with existing and proposed sector-specific cybersecurity legislation, especially for industry sectors such as telecommunications, transport and mobility, energy, and finance. As such, coherence with the existing legislative initiatives is of utmost importance.

Some consulted stakeholders strongly agree with establishing horizontal legislation consistently with NLF provision. Relevant economic operators have long been familiar with the NLF methods and have built up implementation expertise including internal processes, which reduces the effort along the supply chain. These mechanisms are considered both well established and proven effective. Other stakeholders, however, have argued that the Cybersecurity Act (CSA) should rather be placed at the centre of a future European horizontal legislation, as it is already providing cybersecurity requirements linked to assurance levels. The new horizontal act should stipulate the protective goal of ICT security as legally binding, making the schemes of the CSA mandatory.

In the targeted consultation, a similar point was raised among NCAs, some of which judged that the existing CSA already provides for a horizontal framework and simply needs to be better implemented. For some ICT industry players, introducing horizontal legislation would not capture the differences in ICT products when it comes to cybersecurity and the legislation could become quickly outdated while reducing the effectiveness of CSA schemes.

Essential Requirements

The results of the stakeholders' consultation show contrasting stakeholders' opinions concerning the envisaged essential requirements. While most stakeholders agree with the principle of establishing essential requirements for ensuring the cybersecurity of ICT products, some concerns have been raised.

- Manufacturers have argued that it could be beneficial to **map the essential requirements against the existing standards**. The Project Team mapped the Security Requirements (underlying components of the Essential Requirements) to the existing standard, as such, the mapping is already envisaged in the scope of the Study.
- Manufacturers and Consumers Associations highlighted that the essential requirements are **overlapping**. In particular, the first requirement is an overarching one. However, according to the Project Team regrouping all Essential Requirements under the first Essential Requirement would reduce the focus on key security aspects for the product.
- Manufacturers have highlighted that the essential requirements **tackle both products and organisational setups**, and this approach is problematic in the context of the NLF. In this respect, the Project Team identified the difficulty to tackle the security of the product once placed on the market when following strictly the NLF. Particularly, the security of the product itself cannot be achieved without the presence of key organisational processes managed by different stakeholders.
- Manufacturers highlighted that the essential requirements would benefit from mentioning the **secure development lifecycle (SDL),** and Consumers Associations argued the essential requirements would benefit from better underline provisions for **vulnerabilities disclosure.** Both topics, however, are envisaged under the Security Requirements. Therefore, the Project Team believes that they are already covered under the scope of the essential requirements,
- Software developers mentioned that **a longer list would allow for greater flexibility concerning which requirement manufacturer should apply**. This could be problematic. If exceptions to the applications of essential requirements are to be established, they should rather be introduced through conditionalities in the law. The Project Team has so far presented no conditionalities mechanisms for Essential Requirements. On the other hand, the Security Requirements (or similar set of requirements such as harmonised standards

in the NLF) can offer the necessary flexibility to identify the key security measures to apply in order to secure the products.

Based on an initial set of essential requirements prepared by the Project Team, the following conclusion can be drawn: the initial set of Essential Requirements constitute an adequate set of conformity obligations for products, taking also into account the feedback received from stakeholders. Minimal changes in the Essential Requirements, mostly around phrasing, have been provided based on the feedback and replicated in Table 38.

Application of the Essential Requirements to all stakeholders through the product's entire lifecycle (SW designer and developers, manufacturers, vendors, service providers, and operators)

The Essential Requirements as defined in the NLF are addressing manufacturers' only, while other obligations will involve the distributors and importers. However, in the case of ICT Products, this aspect might not fully allow to address Essential Requirements involving not only the phase before the products are placed on the market (pre-market phase) but the entire lifecycle. In the context of this Study, stakeholders have been consulted on the need to address a broader group of stakeholders to fully ensure the security of the product throughout its lifecycle. Particularly, stakeholders were asked whether SW designer and developers, manufacturers, vendors, service providers, and operators should be held responsible together with manufacturers.

The vast majority of consulted stakeholders either agree or strongly agree with the principle that all stakeholders in the value chain should share the burden of responsibilities. There is a vast ecosystem dealing with ICT products and services' cybersecurity, as such, there is a need for a holistic approach, and it is appropriate to envisage obligations for economic operators other than manufacturers. One stakeholder has however flagged that, generally speaking, Directives that are constructed according to the NLF place the responsibility for product conformity essentially on the manufacturer, but any economic operator is considered to be the manufacturer if he changes a product or if the use case results in new or increases an existing hazard.[341] As such, a service provider/software designer can also become the manufacturer in the legal sense under a horizontal NLF.

Several interviewed manufacturers, software developers and service providers underlined the need for including the **users** in the list of relevant stakeholders sharing the responsibilities for products' security. An example that has been offered in this respect by multiple stakeholders is one of the software updates. While the manufacturer or software developer could provide software updates, these actors cannot be regarded as liable if a user, intentionally or unintentionally, fails in installing them. Furthermore, it has been argued that the more general-purpose an ICT product is, the more likely customers are to employ the product in diverse user cases, potentially deviating from the security scenarios and requirements the manufacturer may have anticipated and addressed. As such, mechanisms of **cooperation among manufacturers, operators and users** could be envisaged. For his part, the manufacturer should provide either patches or guidance for the users for a certain defined period. However, after that period expires, he should not be held responsible any longer.

Legally addressing users' responsibilities in the context of Horizontal Legislation would be problematic, if not flawed (e.g., imposing software updates to users). Rather, horizontal legislation should **distinguish between responsibilities in B2B and B2C contexts**. In the first case, shared liabilities can be envisaged. The manufacturer

[341] This holds true as long as the product is once again made available on the market after the changes are being made.

will still play a pivotal role in assessing the conformity of the product, for which he would need to provide corrective measures, such as software updates. Yet, further responsibility of other economic operators might become relevant at the moment they take over control over the product. In a B2C context, instead, the Horizontal Legislation should indirectly address users' responsibilities by **legally limiting manufactures or other subjects' liabilities** in case a product's fault is the result of a users' refusal to perform certain undertakings.

This view has been strongly challenged by interviewed consumers associations. While for all proposed stakeholders a system of joint liabilities should be envisaged, this system should not include users. According to consumers associations, the implementation of security by design and by default should by itself prevent users to undermine the security of the product (e.g., some functions could be designed to avoid users adopting insecure passwords). Consumers buying connected products should be provided with clear information concerning how long manufacturers will provide consumers with security updates and what would happen after that period expires. In this respect, however, other stakeholders highlighted that, as far as the security by design and default is concerned, this would hardly rule out users' responsibilities. Indeed, a **trade-off exists between robustness and usability**, such as that a completely robust application would lose in usability terms. Manufacturers often calibrate secure by default settings to provide the best balance for their largest set of customers. Approaches that require setting the highest level of security possible by default (for example, using the largest possible key sizes for data encryption) can thus create performance and usability issues for users that utilize products in low-risk contexts.

Conformity Assessment

Consulted manufactures, software developers and operators have suggested several issues that should be taken into account when envisaging conformity assessment activities in the context of a Horizontal Legislation.

Firstly, clarity should be provided to which framework a possible Horizontal Legislation would be based upon. If the Horizontal Legislation will be modelled against the NLF, the language should refer to "**declaration of conformity"** rather than to self-assessment or third-party assessment, which is instead used in the context of the Cybersecurity Act. In this respect, according to some stakeholders, the NLF would allow for greater flexibility, while allowing also to cover the entire product life cycle by referring to standards. In particular, referring to the **standard ISA/IEC 62443** allow addressing processes and, thus, the entire product lifecycle.[342]

The legislation should not mandate beforehand which risk profile should be subject to mandatory or non-mandatory involvement of notified bodies. Rather, assessment activities should be carefully selected to fit for the product and assurance level. The appropriate conformity assessment mechanism should hence be **established based on the product's intended use rather than on rigid classifications of the products' risk profiles**. A given product can be associated with several risk levels, depending on the intended use and the operational environment (e.g., private homes vs. critical infrastructure). The decision of the appropriate conformity assessment modules to adopt should be performed on a **case-by-case level.** Unnecessary requirements for the involvement of notified bodies might slower the market and represent an unnecessary burden over some stakeholders (e.g., SMEs).

In particular, SMEs might not have the adequate financial or human resources for perform a conformity assessment with the involvement of an accredited in-house conformity assessment body, or to rely on an external conformity

[342] Notably, not all stakeholders agree on the principle that referring to the NLF would allow to address the whole product life-cycle.

assessment body. Therefore, an horizontal regulation could benefit from envisaging ways to reduce costs that SMEs would face when performing a conformity assessment.

Manufacturers also underlined that not always there are available cybersecurity solutions for flawed systems to be patched. In this respect, the legislation should spell out what the consequences would be in case a fault cannot be mitigated. Specifically, a product should **not be considered faulty in case the cybersecurity default cannot be mitigated**, otherwise, the economic burden of the recall would be on the manufacturer. Besides, a product/solution that has once been placed on the market in compliance with the horizontal legislation should not be considered as legally non-compliant if, at a later point in time, a new (unknown at the time of placing it on the market) attack vector is found. Finally, the Horizontal Legislation should mention that cybersecurity should not be considered a fault in the case, after the inspection, the product does not fulfil the latest stage of cybersecurity requirements, but the existing functions are still acceptable. This holds especially for older technologies that can be considered safe even though they do not fulfil the latest cybersecurity specification.

Operators have highlighted that the **procedures and timing for the ex-post verification** of the products must be better assessed as each security picture has a limited time validity (for example the Pentest). Furthermore, given that few of the activities indicated in the table provide different outputs depending on who performs the checks, it would be beneficial to address **how the different outputs can be compared**.

Interviewed consumers associations stressed instead the need for introducing the concept of continuous conformity applicable to the whole product lifecycle, which would match consumers' expectations. Usually, consumer products tend to be categorised as low-risk profiles, while there are **fundamental risks to human rights related to the use of connected consumer products**. As such, according to consumers associations, to the extent possible, self-assessment should be limited.

Horizontal Legislation and impact on the different stakeholders of the value chain

In terms of the possible impact of a Horizontal Legislation on the different stakeholders, most consulted manufacturers and software developers regard the potential impact as minimal. Most stakeholders declared indeed that, irrespective of the regulatory framework, they have already put in place the envisaged essential requirements. While this holds true, these market players would still favour the adoption of a horizontal legislations as it would better guarantee conscientious vendors against unfair competitions practices.

However, it has been underlined that the potential impact on the stakeholders will also depend on whether there will be consistency with other regulatory instruments. In case multiple pieces of legislation will coexist and overlap incoherently this will represent a huge burden for most companies. In this respect, stakeholders could only benefit from more regulatory certainty provided that there is **coherence with the other verticals of the NLF and with other pieces of legislation** (e.g., RED Delegated Act, Revised NIS Directive).

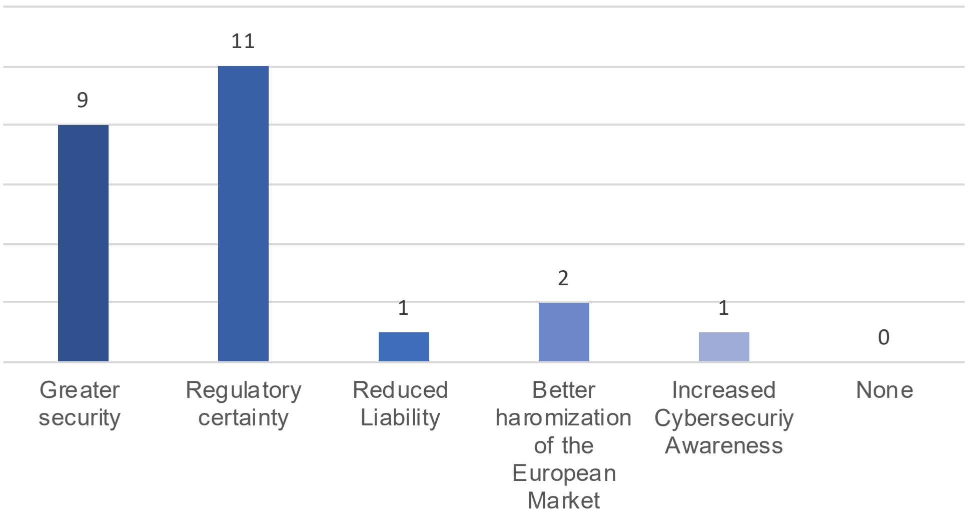
Overall market effects of a Horizontal Legislation

Imposing a Horizontal Legislation would certainly have a relevant effect on the overall ICT market. In this respect, stakeholders have been asked which positive effects and which risks could be envisaged stemming from the implementation of a Horizontal Legislation.

As far as positive effects are concerned, most consulted stakeholders agreed on the idea that establishing a Horizontal Legislation would create greater regulatory certainty and advocate for having one single piece of legislation regulating cybersecurity for ICT products, rather than having a multiplicity of regulations governing the same phenomenon (RED Delegated Act; Machinery Directive; GDPR; etc.).

Greater security in the overall market was also mentioned from several stakeholders among the potential positive effects of a Horizontal Legislation together with a better harmonization of the European market, beneficial for operators aiming at entering the EU market. Figure 41 presents the interviews' results.

Figure 41 Overall positive effects stemming from the implementation of a Horizontal Legislation

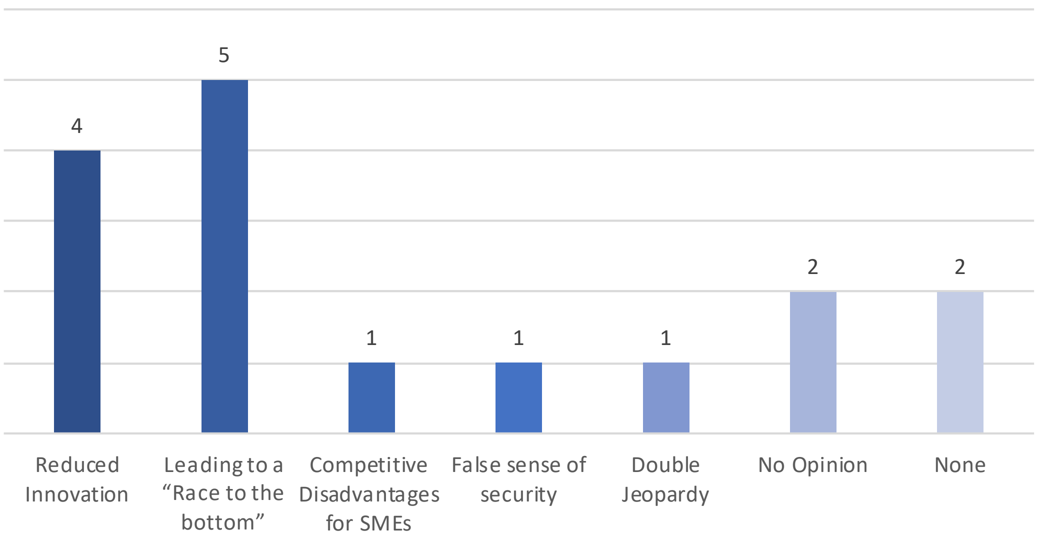


SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), INTERVIEWS, N=14.

When it comes to the risks related to the implementation of Horizontal legislation, the relative majority of stakeholders highlighted that setting minimum requirements will not enable stakeholders to differentiate between various levels of digital security and could lead to "a race to the bottom," with some software producers and developers limiting themselves in adopting baseline security.

However, it has also been argued that a "race to the bottom" might not necessarily occur because companies would always be subject to each-other competition, which would anyway foster their incentives for enhancing their products' performances and functionalities. Furthermore, it has also been argued that even baseline requirements would increase the overall security of all sold products as many of them simply currently do not meet even basic security requirements. Once, the market has settled, it will be possible to raise the baseline and adapt the overall level of security in the EU. Accordingly, set basic security requirements could rather act as a baseline, from which further competition on security as a quality aspect could unfold. Figure 42 shows the interviews' results.

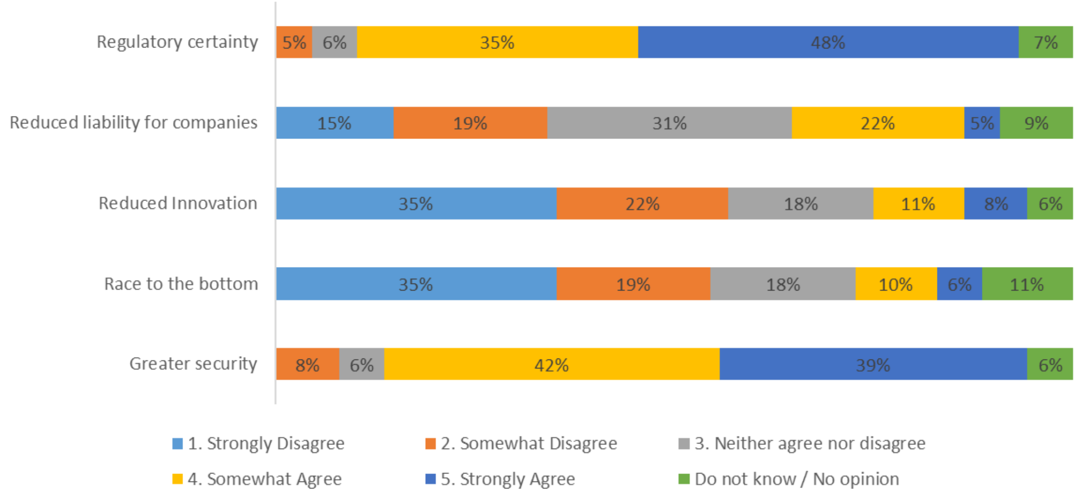
Figure 42 Potential risks stemming from the implementation of a Horizontal Legislation



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), INTERVIEWS, N=14.

A significant majority of the respondents to the targeted consultation agreed that the introduction of horizontal legislation would lead to regulatory certainty (83%) and enhance the security of ICT products (81%). Most respondents disagreed that this policy option would reduce innovation (57%) or cause a 'race to the bottom' (54%).

Figure 43 Opinion of stakeholders on the effect of horizontal legislation



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

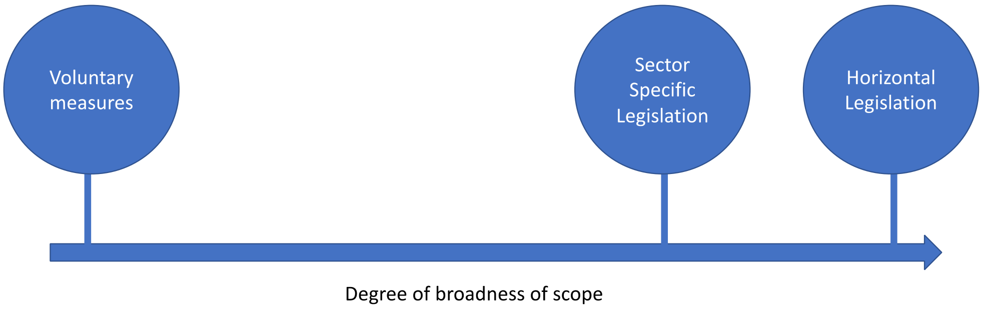
5.2.4 Analysis and specification of Policy Option 3: Sector-specific legislation

Introduction

When the policy options have been presented at a glance, it has been mentioned that they can be divided into two broad categories: voluntary measures and regulatory measures. The regulatory measures differ on the broadness of the scope. The horizontal legislation, already presented, is characterized by the broadest scope since in entails a set of requirements applied to all sectors and categories of products. However, the fear that regulatory intervention could stifle innovation and competition and the awareness that the fast-changing technological landscape of ICT products markets could make a too prescriptive or technical regulation soon obsolete, has suggested also to look for policy options with a more limited scope. This is the case of the **Sector-specific legislation** approach: **the implementation of a common regulatory approach applicable only to specific ICT Product / risk levels or sectors.**

Figure 44 below shows the location of the Sector-specific legislation in the cybersecurity policy options space.

Figure 44 Sector-specific legislation in the cybersecurity policy options space



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Specification of the Sector-pecific legislation

Sector-pecific Legislation is characterized by the implementation of a common regulatory approach applicable only to specific ICT Product / risk levels or sectors. The basic regulatory measures envisaged for the horizontal legislation will still characterize the Sector-specific legislation policy option. The policy option envisages the establishment of a set of essential requirements whose producers and vendors shall comply with, before placing the products on the market and also through the entire product lifecycle; conformity assessment rules (either non- mandatory involvement of notified bodies or mandatory involvement of notified bodies); and market surveillance policies. A detailed description of this measures has already been provided in this report.

Under this policy option, however, these regulatory measures will be applied only to specific ICT products/risk level or sectors. For instance, this policy option could entail requirements such as: No default passwords, implementation of a voluntary disclosure policy and an obligation to keep software updated and could be applied to IoT products for the consumer market only. Based on the input from Task 2 and 3 regarding the analysis of sectors, risk profiles and product categories, the Project Team has envisaged 3 specific types of Sector-specific legislation:

1. **Type one:** Implementation of a common regulatory approach applicable only to specific ICT product categories (Ex: End devices).
2. **Type two:** Implementation of a common regulatory approach applicable only to specific risk levels of ICT product categories (Ex: essential and/or high risk)
3. **Type three**: Implementation of a common regulatory approach applicable only to a specific intended use or sector (Ex: consumer/products/Smart Homes)

The following tables (Table 62, Table 63 and Table 64) specify the characteristics of each type of sector-specific legislation:

Table 62 Sector-specific Legislation Type I

		Policy Option 4
		Sector-specific legislation Type I
		Implementation of a common regulatory approach applicable only to specific ICT product categories (Ex: End devices)
Policy measures		
Essential Requirements		Definition of essential requirements. applied only to a specific ICT product category across all sectors
Conformity assessment	*Non-mandatory involvement of notified bodies*	√
	Mandatory involvement of notified bodies	√
Life cycle		√
Risk Profiles	*all*	√
	some	
Product/Sector categories	*all*	
	some	√
Market surveillance		√

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

Table 63 Sector-specific Legislation Type II

		Policy Option 4
		Sector-specific legislation Type II
		Implementation of a common regulatory approach applicable only to specific risk levels of ICT products categories (Ex: essential and/or high)
Policy measures		
Essential Requirements		Definition of essential requirements. applied only to a specific ICT product category across all sectors
Conformity assessment	*Non-mandatory involvement of notified bodies*	√

	Mandatory involvement of notified bodies	√
Life cycle		√
Risk Profiles	*all*	
	some	√
Product/Sector categories	*all*	√
	some	
Market surveillance		√

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors’ own elaboration based on literature review and data collection activities.

Table 64 Sector-specific Legislation Type III

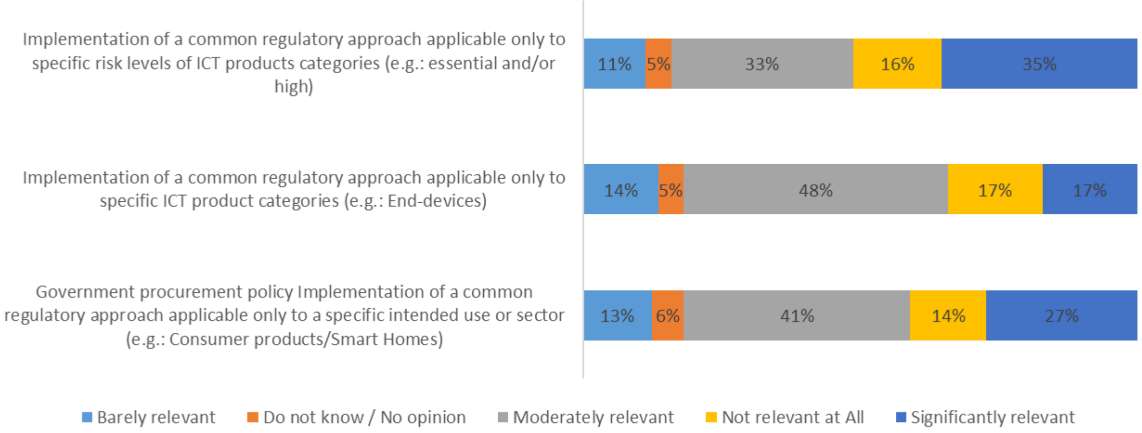
		Policy Option 4
		Sector-specific legislation Type III
		Implementation of a common regulatory approach applicable only to a specific intended use or sector (Ex: Consumer products/Smart Homes)
Policy measures		
Essential Requirements		Definition of essential requirements. applied only to a specific ICT product category across all sectors
Conformity assessment	*Non-mandatory involvement of notified bodies*	√
	Mandatory involvement of notified bodies	√
Life cycle		√
Risk Profiles	*all*	√
	some	
Product/Sector Categories	*all*	
	some	√
Market surveillance		√

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors’ own elaboration based on literature review and data collection activities.

During the third workshop, held on the 4th of February with 126 participants and focused on the policy options, participants have been asked which Type of sector-specific Legislation would be the most appropriate to address the need for cybersecurity of ICT products. The participants’ answered with a relative preference for *Type 2: Implementation of a common regulatory approach applicable only to specific risk levels of ICT products categories* (Ex: essential and/or high) (25 out of 126 participants, or 20%).

The targeted consultation mirrors this finding. Of the three types of sector-specific legislation put forward, the implementation of a common regulatory approach applicable to only specific risk levels of ICT product categories was deemed the most relevant by 35% of the respondents.

Figure 45 Which of the following Sector-Specific Legislation types would be the most relevant to address the need of cybersecurity of ICT products?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Respondents on behalf of the ICT industry suggest that addressing cybersecurity requirements based on risk level is common practice and most effective as low-risk products do not need to have the same regulatory requirements as products with a higher risk level. However, some regulation is also needed for low-risk products.

Nevertheless, shortcomings stemming from the implementation of a common regulatory approach applicable to specific risk levels of ICT products were also highlighted. Particularly, the challenge with the identification of risk levels lies with the interpretation of competent authorities and/ or of conformity assessment methods to identify what constitutes an essential or high risk vs. lower-risk applications.

More generally, while according to some participants at the third workshop, sector-specific legislation would allow to better tackle highly critical sectors, most participants mentioned that sector-specific regulation should be avoided as it leads to non-coherent requirements among sectors and could become problematic for manufacturers serving several sectors.

The targeted consultation complements and confirms this evaluation. Among ICT industry players judging that this policy option would not address the need for cybersecure ICT products, a recurrent point made is that sector-specific legislation creates a complex legal architecture, with risk of market fragmentation, confusion and inconsistent or overlapping security requirements. This view was echoed by two associations representing professional users. In addition, both these associations argued that sector-specific security requirements should not be part of legislation but should instead be left to widely accepted proven international standards to keep legislation technology-neutral and account for differences across sectors.

NCAs in favour of this policy option also often acknowledged the market fragmentation risks it poses but argued that sector-specific legislation should only cover the specific security needs of critical sectors while horizontal legislation should be the centrepiece addressing key cybersecurity issues. In particular, some NCAs argued that horizontal legislation will make it possible to set a generic rule without precisely managing the requirements necessary for good protection, which means that complementary sector-specific regulations may be necessary. The reason given is that essential requirements may not be sufficiently forward-looking to ensure all ICT product types can be future proofed given their specific risk profiles.

Overall, while sector-specific legislation might be unavoidable in certain circumstances (such as medical devices), its application should be limited, or envisioned as complementing a horizontal legislation. Ideally, all ICT products should be considered as potentially equally sensitive for security purposes, unless and until a risk-assessment is performed. Excessive recourse to sector-specific legislation would increase fragmentation and might end up in continuous interpretations and revisions of their scope of applicability, especially as ICT products and services increasingly overlap. Besides, sector-specific legislation might not consider the possible horizontal usage of ICT products in fields of application that per se might pose higher risks than those related to the originally intended field of use.

The UK case as sector-specific legislation of Type three

The UK government started suggesting a voluntary approach to manage the security of the Consumer IoT product market through the publication in 2018 of a Code of Conduct for IoT Consumer products. Recently, DCMS moved toward a minimum set of requirements mandatory by law (Consultation in July 2020). The UK moved from a voluntary approach to more legally binding measures due to growing evidence suggesting that good practices were not being implemented. Indeed, when the UK published the Code, it monitored the adoption of the good practices shared also with ETSI. While the hope was that these good practices would have been enough, by keeping monitoring their adoption, the UK realized that a more horizontal approach was needed. Therefore, the DCMS decide to make legally binding the following measures in the UK:

- *No default passwords:* All IoT device passwords shall be unique and not resettable to any universal factory default value.
- *Implement a vulnerability disclosure policy:* All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.
- *Keep software updated:* Software components in internet-connected devices should be securely updateable

In choosing the three requirements the UK adopted a pragmatic approach: define which requirements would allow gaining the best possible outcome in terms of both security and consumers' protection while reducing the burden as much as possible on industries. These three requirements have a set of useful characteristics:

- They are not fully binary but pretty close to be binary (you either report vulnerabilities or you don't) and, as such, they are immediately testable.
- They avoid having requisites that would have necessitated themselves another layer for being tested.

Furthermore, the UK had a consultation in which it was proposed to either mandate all the thirteen components of the Code of Practice or to mandate only the top three aspects of the Code:

- There was strong support for having those three aspects being the first baseline against which to draft the regulatory requirements

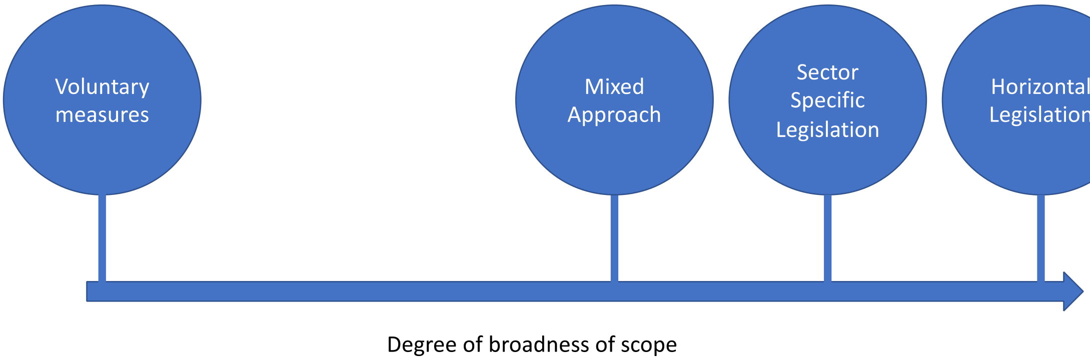
- There was almost universal support in terms of regulating the IoT Consumer products market and not leaving it to voluntary measures only.[343]

5.2.5 Analysis and specification of Policy Option 4: Mixed approach

Introduction

As requested in the terms of reference of the study and also to allow for more flexibility and a better fit to ad hoc situations, the Project Team has designed an approach that contemplates regulatory and co-regulatory measures: the **mixed approach. This approach is characterized by a combination of regulatory and voluntary measures.** Figure 46 below shows the locus of the mixed approach in the cybersecurity policy options space.

Figure 46 Mixed Approach Option in the Cybersecurity Policy Space



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Specification of the Mixed Approach

The Policy Option Mixed Approach is characterized by a combination of regulatory and voluntary measures. As for the case of the Sector-specific Legislation, the basic regulatory measures envisaged for the horizontal legislation will still characterize the mixed-approach policy option. The policy option envisages the establishment of a set of essential requirements whose producers and vendors shall comply with, before placing the products on the market and also through the entire product lifecycle; conformity assessment rules (either non- mandatory involvement of notified bodies or mandatory involvement of notified bodies); and market surveillance policies. A detailed description of this measures has already been provided in this report.

In the mixed approach, these regulatory measures are complemented with some of the voluntary measures previously described. For instance, this option could mandate a set of minimum requirements for some products and

[343] This section draws from the meeting of the Project Team with representatives of the UK DCMS.

suggest labelling systems for some others. Hence, it combines minimum measures with the possibility – for risker products – to enhance the level of security through voluntary measures.

Based on the input from Task 2 and 3 regarding the analysis of sectors, risk profiles and product categories, the Project Team has envisaged 2 specific types of mixed approach:

- **Type one:** Implementation of a combination of regulatory and voluntary measures applicable to all categories and risk profiles of ICT products
- **Type two**: Implementation of a combination of regulatory and voluntary measures applicable only to a specific intended use or sector (Ex: Smart Homes)

The following tables specify the characteristics of each type of Mixed approach:

Table 65 Mixed Approach Type I

		Policy Option 5
		Mixed Approach Type I
		Implementation of a combination of common regulatory approach applicable to all categories and risk profiles of ICT products + non-regulatory measures
Policy measures		
Essential Requirements		Definition of essential requirements. applied only to a specific ICT product category across all sectors
Conformity assessment	*Non-mandatory involvement of notified bodies*	✓
	Mandatory involvement of notified bodies	✓
Life cycle		✓
Risk Profiles	*all*	✓
	some	
Product categories	*all*	✓
	some	
Market surveillance		✓

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

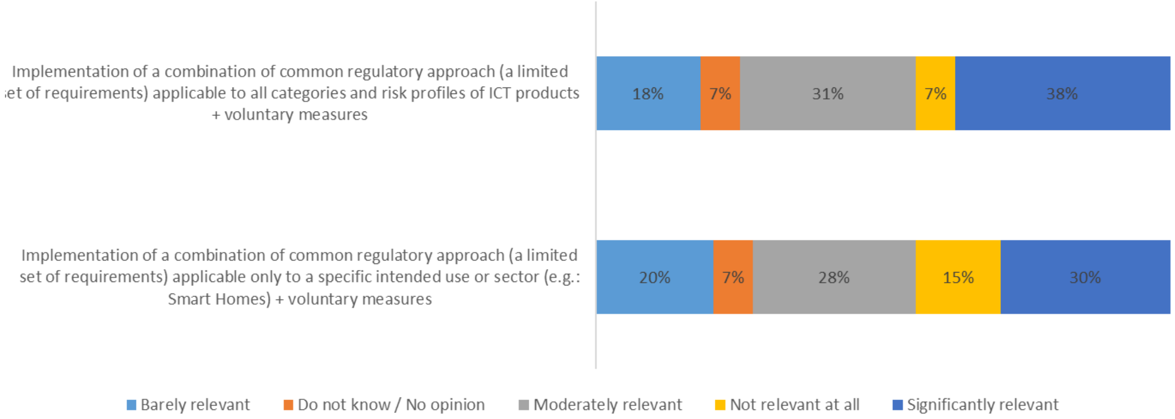
Table 66 Mixed Approach Type II

		Policy Option 5
		Mixed Approach Type II
		Implementation of a combination of common regulatory approach applicable only to a specific intended use or sector (Ex: Smart Homes) + non-regulatory measures
Policy measures		
Essential Requirements		Definition of essential requirements. applied only to a specific ICT product category across all sectors
Conformity assessment	*Non-mandatory involvement of notified bodies*	✓
	Mandatory involvement of notified bodies	✓
Life cycle		✓
Risk Profiles	*all*	✓
	some	
Product/Sector categories	*all*	
	some	✓
Market surveillance		✓

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

When asked which type of Mixed Approach would be the most appropriate to address the need for cybersecurity of ICT products, results of the targeted consultation show that, for respondents, a mixed approach combining regulation applicable to all categories and risk profiles of ICT products and voluntary measures would be more significantly relevant than a mixed approach combining regulation applicable to specific ICT products and voluntary measures (38% vs. 30% of the total respondents).

Figure 47 To what extent would the following mixed approach types be relevant to address the need of cybersecurity of ICT products?



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

Some ICT industry players highlighted that the common regulatory approach within a mixed approach type 1 might be the more favourable option, but it still would be subpar compared to a horizontal approach and it would also add unnecessary complexity, potential for confusion and potentially inefficiency.

Among NCAs and European institutions, support for mixed approaches was marginally higher compared to ICT industry players. It was argued that mixed approaches could be an effective response to the dynamic nature of ICT products, services and cyber threats by including a set of more detailed and adaptable rules. For NCAs and European institutions in favour of this policy option, a key point is that it would offer some flexibility in adaptation as different parts of the ICT market require a different approach due to varying levels of cybersecurity maturity. More specifically, a mixed approach would complement necessary regulation with voluntary measures to support market forces towards greater cybersecurity.

Also, according to some participants at the third workshop, the mixed approach might allow to better tackle highly critical sectors. The rationale for this argument stems from the idea that a product that was originally developed for a certain intended use could still be adopted in other, possibly riskier sectors.

On the other hand, the most frequent argument shared by ICT industry players and professional users who judge this policy option as not addressing ICT cybersecurity effectively, is that a mixed approach will only introduce more fragmentation in the ICT sector, greater legal uncertainty and confusion for both end-users and economic operators and result in additional costs for everyone. Particularly, additional costs for manufacturers might arise from the need to employ both experts on compliance and voluntary schemes.

The Singapore Case as example of type II Mixed approach

In October 2020, the Cyber Security Agency (CSA) of Singapore has introduced the Cybersecurity Labelling Schemes for home routers and smart home hubs. The labelling initiative is voluntary and comprises four levels of rating based on the number of asterisks, each indicating an additional tier of testing and assessment the product has gone through. The scheme aims to motivate manufacturers to develop more secure products, moving beyond designing such devices to optimise functionality and cost. Level One, for instance, indicates that a product meets basic security requirements such as ensuring unique default passwords and providing software updates, while a level four product has undergone structured penetration tests by approved third-party test labs and fulfilled level three requirements

At the same time, the Infocom Media Development Authority (IMDA) has decided to **mandate a set of minimum-security requirements for home routers starting from 13 April 2021.**

The enhanced security requirements include:

- randomised and unique login credentials for each device
- minimum password strength
- disabling system services and interfaces that are deemed to be vulnerable
- default automatic downloads of firmware updates for security patches
- secure authentication of access to the device's management interface and
- validation of data inputs to the device to safeguard against remote hacking

On the 21 of January 2021, the CSA of Singapore has widened the cybersecurity labelling initiative to include all consumer Internet of Things (IoT) devices such as smart lights, smart door locks, smart printers, and IP cameras.

The scheme, which initially applied only to Wi-Fi routers and smart home hubs, rates devices according to their level of cybersecurity features. Wi-Fi home routers that comply with IMDA's specifications would also meet Level 1 of the CLS which was recently introduced by the Cyber Security Agency of Singapore. Home routers, as well as smart home hubs, that are assessed to be secure and compliant will bear these labels.[344] The IoT requirements as described in the Singapore model are similar to the UK Consumer IoT essential requirements.

5.3 Comparison among the policy options

Table 67 presents the comparison among the policy options Horizontal legislation, Sector-specific (Type1,2,3) and Mixed approach (Type 1, 2) and clearly shows the differences based on the various degree of broadness of scope.

Table 67 Mapping of the Differences among policy options

		Horizontal Legislation	Sector-specific Type 1	Sector-specific Type 2	Sector-specific Type 3	Mixed Approach Type 1	Mixed Approach Type 2
Risk Profiles	*All*	✓	✓		✓	✓	✓
	Some			✓			
Product/Sector Categories	*All*	✓		✓		✓	
	Some		✓		✓		✓
Lifecycle Approach		✓	✓	✓	✓	✓	✓
Essential Requirements		✓	✓	✓	✓	✓	✓
Conformity Assessment	*Non-mandatory Involvement of Notified Bodies*	✓	✓	✓	✓	✓	✓
	Mandatory Involvement of Notified Bodies	✓	✓	✓	✓	✓	✓
Market Surveillance		✓	✓	✓	✓	✓	✓

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

During the third workshop, participants have been asked which of the proposed policy options would overall better address the needs of cybersecurity for ICT products. *Policy option 2 Horizontal legislation* has been the most voted (37 out of 123 respondents, or 30%)[345], while the second most preferred option has been *Policy Option: Mixed approach* (20 out of 123 participants, or 16%).

The results of the forthcoming Targeted Consultation provided additional information on the policy options preferences of the different stakeholders. Interestingly, respondents were overall most likely to indicate that a mixed approach would best address the need for cybersecurity requirements for ICT products. Horizontal legislation is the second-best option according to the overall response.

[344] See Yu Eileen (2021), "Singapore widens security labelling to include all consumer IoT devices, ZDNet, https://www.zdnet.com/article/singapore-widens-security-labelling-to-include-all-consumer-iot-devices/#ftag=RSSbaffb68

[345] The participants of the Workshop n.3 were 126, however, the respondents of this poll were 123. Three participants left the virtual meeting before the polling was launched.

Table 68 Which of the proposed policy option would address better the need for cybersecurity requirements for ICT products?

Policy Option	No. of respondents	% respondents
0 – Baseline / No action	2	2%
1 – Voluntary measures	2	2%
2 – Horizontal legislation	25	28%
3 – Sector-specific legislation	24	27%
4 – Mixed approach	32	36%
Do not know / No opinion	3	3%

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

This result should be analysed bearing in mind that the type of Mixed Approach considered to be the most appropriate to address the need for cybersecurity of ICT products is the one combining regulation applicable to all categories and risk profiles of ICT products and voluntary measures. Hence, respondents advocate for horizontally establishing a minimum set of requirements, while acknowledging that other non-mandatory measures could help in addressing the broader set of issues that relates to ICT security. For example, for a specific community of users, there might be a need for further security reassurance on top of the horizontal requirements, which would not make sense to impose on the rest of the market because they are relevant only for that specific segment of users. A mixed approach could, hence, combine minimum measures with the possibility – for risker products – to enhance the level of security through voluntary measures.

In support of Policy Option 2 – Horizontal Legislation, NCAs suggested that this approach should have a clear hierarchy based on intended use, reducing the risk of legal uncertainty by following NLF elements. Delegated acts may update the horizontal regulation with respect to new developments. In cases where a vertical refinement of regulation is not desired, a horizontal approach would steer the market forces towards greater cybersecurity. In this respect, it should be noted that some NCAs argued that horizontal legislation will make it possible to set generic rules, while vertical refinements could be guaranteed through the adoption of sector-specific regulation rather than voluntary measures.

5.4 Mapping of policy options against problem drivers and policy objectives

Based on the information collected to date, desk research, as well as preliminary feedback from the third workshop and the online interviews, using a Likert scale from 1 to 5 (1= Not at all, 2= To a limited extent, 3= To some extent, 4= To high extent and 5= To the fullest extent), the Project Team mapped the policy options against the problem drivers and the policy objectives, and calculated the score for each policy option.

Table 69 presents the score of the mapping of each policy option against the problem drivers and Table 70 below shows the score of the mapping of each policy option policy against the objectives.

Table 69 Mapping of the Policy Options Against the Problem Drivers

	Policy Options				
Problem Drivers	**Policy Option 0: Baseline**	**Policy Option 1: Voluntary Measures**	**Policy Option 2: Horizontal Legislation**	**Policy Option 3: Sector-specific Legislation**	**Policy Option 4: Mixed Approach**
No mandatory Requirements (e.g. no clear obligations for the manufacturer)	0	0	5	4	4
No common legal basis that sets cybersecurity requirements for ICT products	0	0	5	4	4
No rules for post-market surveillance	0	1	5	4	3
No clear cybersecurity risk assessment model at EU level.	0	1	5	5	3
No harmonized conformity assessment across the EU	0	3	5	5	5
No harmonized security by design principles at national level to increase the security of ICT products	0	0	5	3	3
Cybersecurity for ICT products has a high cost for the manufacturer	0	5	2	2	3
Insufficient use of certification by the manufacturer	0	3	5	3	3
No evident competitive advantages derived from cybersecurity	0	3	5	3	3
No incentives for the manufacturer to make the product more secure	0	4	5	3	3
Cybersecurity not addressed in all stages of the product lifecycle (design, development, delivery, maintenance)	0	3	5	5	5
Manufacturers tend to care more for sales than security	0	2	4	4	4
Low cooperation among Member States to define a common baseline for cybersecurity	0	2	5	3	3
Cybersecurity becomes a barrier rather than an enabler for the manufacturer	0	4	4	3	3
Cybersecurity requirements for ICT products differ across application domains	0	0	5	5	5
Lack of qualified security professionals (i.e. developers)	0	4	2	2	2
Cybersecurity aspects not sufficiently covered in technical studies curricula.	0	5	2	2	2
No clear definition of the main requirements to ensure the appropriate	0	0	5	5	5

(and minimum) level of security of an ICT product					
No available information for the cybersecurity properties of an ICT product	0	3	5	3	3
No methods to communicate the security level of an ICT product to the consumers	0	4	4	4	4
Information asymmetry – the cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons)	0	2	4	2	2
Security of an ICT product is expected by default	0	0	5	0	3
No common understanding between the manufacturer and the user of what a secure ICT product is	0	4	4	4	4
No skills of the users to use ICT products safely (e.g. passwords)	0	3	5	3	3
Total	**0**	**56**	**106**	**81**	**82**

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCT (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES

Table 70 Mapping of the Policy Options Against the Policy Objectives

Policy Options	Increase the level of cybersecurity of ICT products in the EU
Policy Option 0: Baseline	0
Policy Option 1: Voluntary Measures	2
Policy Option 2: Horizontal Legislation	5
Policy Option 3: Sector-specific Approach	3
Policy Option 4: Mixed Approach	4

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Based on desk research analysis and the stakeholders' feedbacks collected through the third workshop, the performed interviews, and the targeted consultation, the Project Team preliminary evaluation suggests that *Policy Option 2: Horizontal Legislation* should be preferred over the other options.[346]

Horizontal Legislation would allow to harmonize the EU regulatory landscape and avoid overlapping requirements stemming from different pieces of legislation. Besides, Horizontal legislation could create greater security in the overall market as well as a better harmonization of the European single market, creating more viable conditions for operators aiming at entering the EU market.

Furthermore, Horizontal legislation would allow to better tackle the problem drivers compared to the other policy options. For example, Horizontal legislation allows addressing the absence of mandatory requirements (e.g., no clear obligations for the manufacturer), or the absence of rules for post-market surveillance, with regards to cybersecurity.

[346] Results from the targeted consultation suggested a slightly stronger preference of the respondents for the Mixed approach. Nonetheless, the results between the Horizontal Legislation and the Mixed Approach were very close, with a clear preference for Horizontal Legislation when it comes to the Impact Assessment, as it will be outlined in the next chapter.

6 Analysis of the possible impacts

This Section aims to assess impacts for each policy option following the criteria set out in Table 71 below, building on desk research and responses from Delphi panel. It presents results for each assessment criteria (effectiveness and social impacts, efficiency and economic impacts, coherence, fundamental rights, EU added value and environmental impact) and undertakes comparative assessment of policy options.

The comparative analysis finds that the Horizontal legislation (Policy Option 2) scores the highest on most assessment criteria, followed by the Sector-specific legislation (Policy Option 3) and the Mixed approach (Policy Option 4). Voluntary measures (Policy Option 1) and the No action (Policy Option 0) score the lowest.

Table 71 Criteria for comparative assessment of policy options and mapped impacts

Criteria	Impacts mapping
Effectiveness and social impacts	Outcomes related to the six specific policy objectives.
	Social impacts • The level of cybersecurity of ICT products. • Material and non-material safety (e.g. life, health, financial loss). • The choice of reliable and secure ICT products. • The trust in ICT products and the Digital Single Market.
Efficiency and economic impacts	Macro-economic • Improved functioning and harmonisation of the Internal Market due to potential regulation. • Improved fairness in competition in the Internal Market due to potential regulation – level playing field avoiding the creation of national legislation on ICT products cybersecurity. • Stimulation of the development of the Digital Single Market due to potential regulation improving cybersecurity in ICT products. Micro and meso-economic • Impact on costs due to potential regulation. • Cost-effectiveness of the potential regulation. EU Industry • Impact on competitiveness of EU industry due to potential regulation. • Impact on innovation in the ICT industry
Coherence	Coherence w ith other EU and national initiatives.
Fundamental rights[347]	Protection of personal data. Consumer protection. Protection of liberty and security.
EU added value	EU added value compared to Member States acting separately.
Environmental impact	Reduced risk of environmental damage related to cyber incidents in ICT products.

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

[347] Fundamental rights as formulated in the CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

6.1 Effectiveness and social impacts

This Section assesses how the policy options perform in terms of the expected outcomes (specific policy objectives) and other social impacts. The evidence presented in this Section on effectiveness is mostly qualitative.

Table 72 outlines **the specific policy objectives (SPOs)** and the extent to which the policy options are likely to meet them. Quite importantly, this can be considered – at this stage – as a theoretical exercise as it is not possible to know how each policy would look like in detail. Thus, it is only possible to indicate the extent to which each policy options could potentially include and address specific objectives.

With this caveat in mind, Policy Option 2 (Horizontal legislation) and Policy Option 4 (Mixed approach) seem to be the most impactful options to address most of the SPOs. However, the precise impact depends on the specificities of the legislation and measures underpinning both options. For example, while it is likely both options will set a common legal basis defining mandatory requirements, certification processes, risk assessment models and post market surveillance mechanisms (SPO1), they might not regulate cybersecurity curricular programmes for professional users (SPO5).

In contrast to Option 2 and Option 4, Policy Option 1 (Voluntary measures) and Policy Option 3 (Sector-specific legislation) are likely to address the SPOs only to some extent. This is because the effect depends on voluntary measures which could result in weak compliance or specific sectors and products being out of coverage.

Table 72 Specific policy objectives and policy options

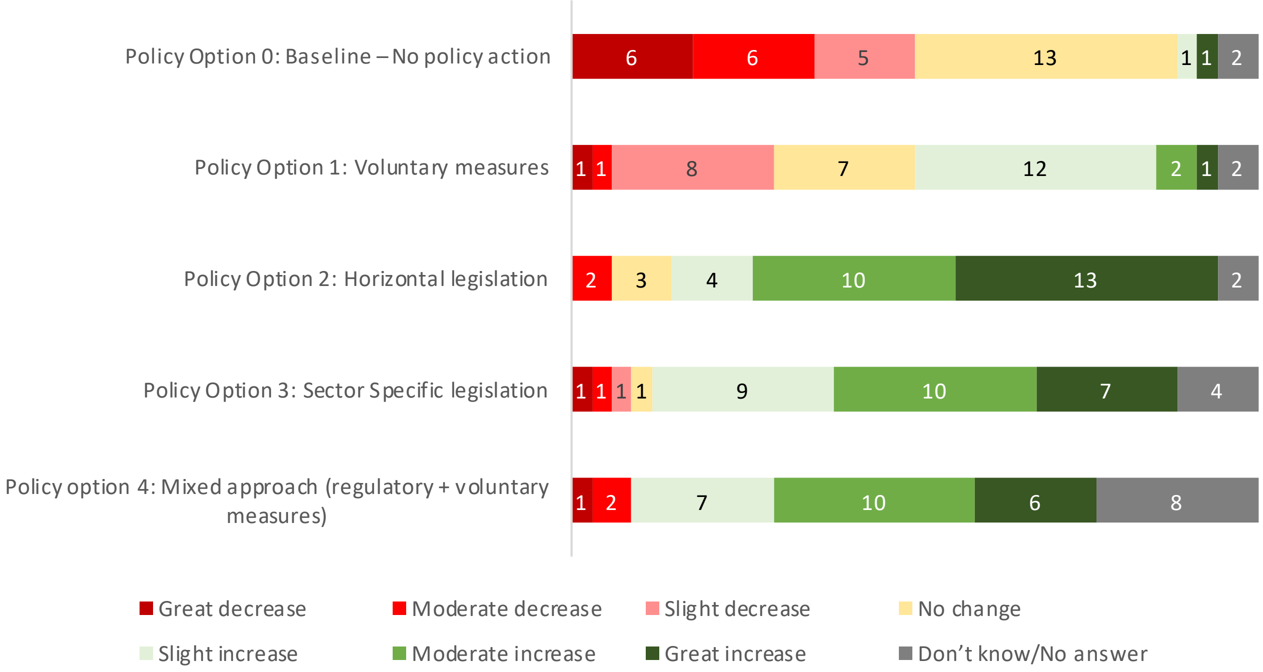
Specific policy objectives	Policy Option 0	Policy Option 1	Policy option 2	Policy option 3	Policy option 4
SPO 1 Set a common legal basis defining mandatory requirements, certification processes, risk assessment models and post market surveillance mechanisms	-	Partly	Fully	Partly	Fully
SPO 2 Define a mechanism that incentives manufacturers to produce more secure ICT products	-	Partly	Fully	Partly	Fully
SPO 3 Address cybersecurity at early stages of product development	-	Partly	Fully	Partly	Fully
SPO 4 Define comprehensive cybersecurity requirements for ICT products across all application domains.	-	Partly	Partly	Fully	Partly
SPO 5 Promote cybersecurity curricular programmes for professional users	-	Fully	Partly	Partly	Fully
SPO 6 Setup a method to inform consumers about the security level of ICT products	-	Partly	Fully	Partly	Fully

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Impacts of policy options on the level of cybersecurity of ICT products

Concerning the overall **level of cybersecurity of ICT products in the EU**, stakeholders expect that horizontal legislation will be the most impactful followed by the Sector-specific legislation and mixed approach (Figure 48). Voluntary measures are likely to have a slight impact, while the business-as-usual scenario (No policy action) is expected to result in a decrease in the level of cybersecurity.

Figure 48 Impact on the level of cybersecurity of ICT products in the EU



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

Concerning **taking no policy action**, stakeholders believe that the digital sector and ICT technologies would continue to expand into all sectors and products, and thus the level of cybersecurity would decrease over time if nothing is done. Business as usual would also lead to stagnation on the development of security for ICT products resulting in a fall in cybersecurity.

Voluntary measures might result in slight increase in the level of cybersecurity because it is expected that the manufactures who already mind cybersecurity of their products will adopt measures on voluntary basis. Perhaps a slight peer-pressure or rising customer expectations would yield slightly higher levels of cybersecurity. However, it risks creating further fragmentation of the single market. Mindful manufacturers would see themselves in increased competition against manufacturers (often from third countries) who would take no action. Therefore, it seems that a regulation would be the most effective strategy. A regulation seems to be welcome mostly for the equal treatment in the application regardless of any increase in administrative burden. Stakeholders manifested that cyber-attacks and the management of personal data have become a major issue that must be regulated in the best possible way.

Among all the regulatory frameworks, horizontal legislation received the most support among stakeholders. The impact of mandatory horizontal requirements on cybersecurity would be the highest as it covers all connected products, thereby also ensuring a high-level of consumer protection. It is expected to yield the highest results because on the one hand it sets a ground level for security of products and on the other hand, especially if established in the NLF, gives opportunity for a (possible fine grained) staggered approach, concerning different modules for example. In addition, if it is based on the NLF, horizontal legislation can be implemented faster by manufactures since they are already familiar with the framework. The biggest advantage of a horizontal approach is thought to be that it avoids patchwork and overlapping or inconsistent requirements. Hence, new cybersecurity requirements can scale faster and broader.

Stakeholders from the industry expressly supports mandatory and horizontal cybersecurity requirements based on the principles of the NLF. The increasing spread of digital technologies is creating a wide range of new opportunities – for both private and commercial users. At the same time, digitalisation also poses numerous challenges in terms of safety and security as well as privacy, which can lead to additional risks. These risks can be mitigated by employing targeted technical, regulatory, and behavioural measures (such as security by design). The remaining residual risks can be reduced accordingly by applying state of the art measures to strengthen resilience. A high degree of cyber resilience is a basic prerequisite for the trouble-free functioning of highly digitalised processes, connected products and services. Coherent legal provisions are the key to maintaining the international competitiveness of the European industry. Laws and harmonised European technical standards (hEN) must go together to meet the dynamic requirements for enhanced cyber resilience. Stakeholders stressed that when further regulating the cyber-resilience of products and services, the EU Commission must avoid the creation of a regulatory hotchpotch. Only a horizontal NLF-based approach can help in avoiding such a situation.

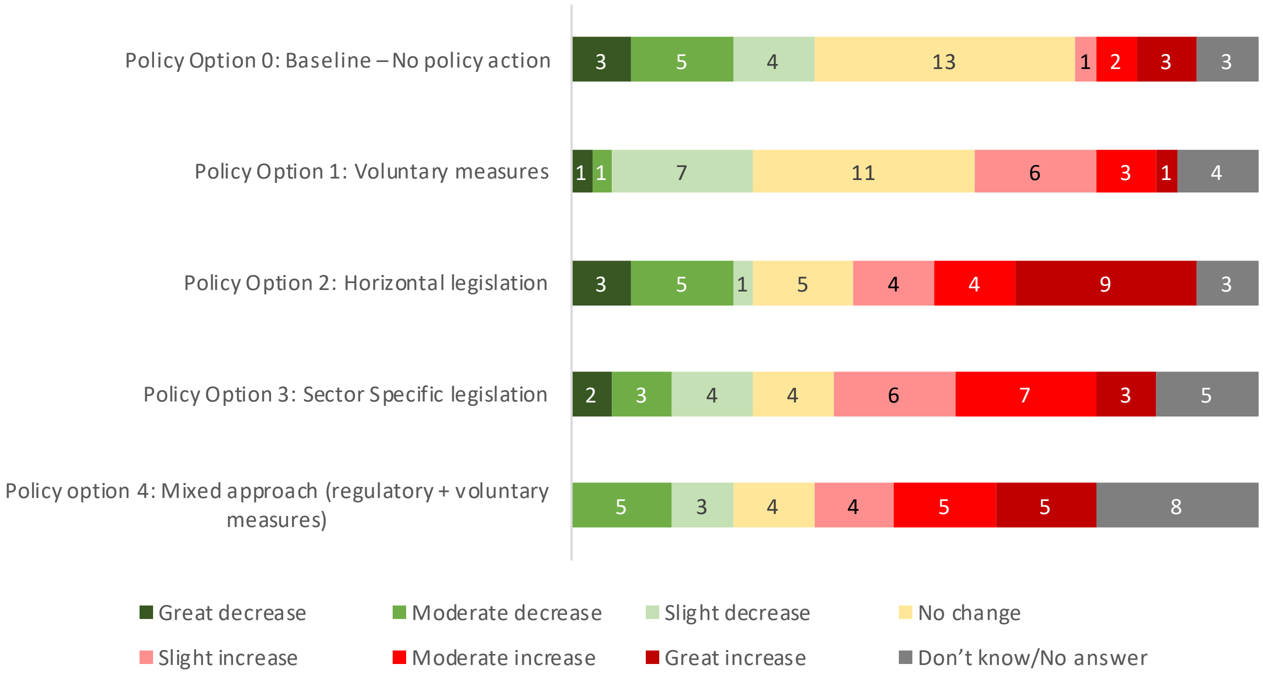
Nevertheless, a one-size-fits-all approach towards harmonisation cannot be effective beyond setting the lowest common denominator of requirements because of the increasing diversity of connected devices. Horizontal legislation should be carefully scoped to avoid the risk of introducing any overlap with existing and proposed, sector-specific cybersecurity legislation, especially for industry sectors such as telecommunications, transport and mobility, energy, finance, and healthcare.

Sector-specific legislation and mixed approaches were considered by stakeholders as having the disadvantage of a possible fragmentation. In some specific cases, it could be useful to set some Sector-specific legislation on top to ensure the very Sector-specific security needs. In Sector-specific legislation, the cybersecurity level would increase somewhat, but conflicting with other measures nullifying the efforts. This effect may end up in a waste of resources. Mixed approach is expected to increase cybersecurity in a moderate or great extent depending on which specific regulatory measure is adopted. For example, a horizontal NLF-approach in a mixed approach could yield the same results as a horizontal legislation.

Impact of the policy options on material and non-material safety

Concerning the impact of the policy options on **material and non-material safety** (e.g. life, health, financial loss) **stakeholders expect that horizontal legislation will have the greatest impact** on safety, followed by Sector-specific legislation and Mixed approach (Figure 49). Voluntary measures are likely to have no change while the business as usual (No policy action) is most likely to decrease the level of material and non-material safety.

Figure 49 Impact on material and non-material harm to safety



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

In the case of No policy action, increased penetration of digital technology will create economic and safety issues. Insufficient regulation or voluntary measures only with very weak legal and practical protection of equipment owners (B2C, B2B, B2A) may result in rising the number of problems and security breaches. There are mainly two issues: manufacturers hide behind a chain of companies and suppliers and the liability for IoT software vulnerabilities based on Council Directive 85/374/EEC [348] that covers only B2C even if the real users are customer who uses medical, network or another connected equipment.

Horizontal legislation or "horizontal" in the Mixed approach would raise the overall level of cybersecurity, therefore making life for cyber-criminals harder. For example, to extort money, especially since important tools for cyber-criminals, like botnets are harder to establish and use, if the overall resilience level is higher. A core challenge for horizontal legislation or standards is the prioritization of essential requirements. For example, a manufacturer has responsibility to enable the foundation of cybersecurity through risk-based methodology according to a threat model that is agnostic to services running on those products. Although any minimum set of security requirements for a product is necessary to be offered to service providers, the services may be beyond the responsibility of the product manufacturer. Stakeholders highlighted that there should be a balance between complexity of the supply chain and innovation of new products on the market. Assessment methodologies applied universally across the market will require harmonization of the respective standards across all products. Assessment activities should be carefully

[348] This refers to Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

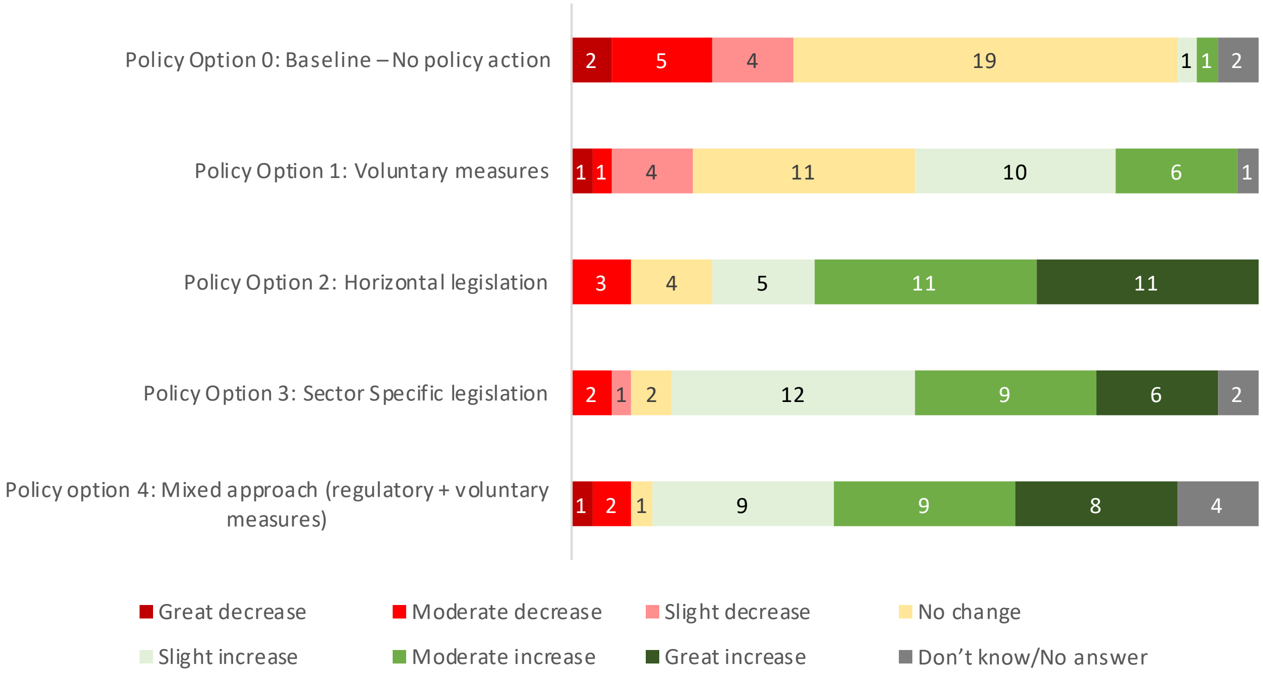
selected to fit for the product and assurance level. As regards assurance, a basic level of security with self-assessment may involve third-party evaluation. Stakeholders stressed the importance to consider the difference between certification and evaluation or assessment activities. Many manufacturers of connected devices use external, third-party assessment as part of product cybersecurity separately from certification activities, which may be useful to increase the security level of their products independently from certification.

A sector-specific legislation could leave a lot of blind spots, therefore not really raising the resilience level. Additional sector-specific legislation or requirements based on the intended use of the technology could create overlaps and duplication of compliance requirements for ICT providers, which could have an adverse effect on the sought regulatory impact.

Impact of the policy options on the choice of reliable and secure ICT products

Concerning the impact of the policy options on **the choice of reliable and secure ICT products**, the results are similar to previous impacts, with stakeholders expecting Horizontal legislation to be the most impactful, followed by Mixed approach and Sector-specific legislation (Figure 50). Voluntary measures are likely to have slight to moderate increase while No policy action would have no change.

Figure 50 Impact on the choice of reliable and secure ICT products



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Delphi panel, N=34

When prompted to elaborate on their answers…

For most respondents, the rationale was similar with increasing the overall level of cybersecurity. In the long term, having No policy would lead to decrease in the choice of reliable ICT products, Voluntary measures would promote a slight increase, especially if the awareness of the consumers rises. A Horizontal legislation and "horizontal" legislation in the Mixed approach would set a minimum threshold for products entering the market, therefore only allowing products into the market which possess an adequate level of security. Sector-specific legislation would only raise the security requirements for products in some areas and could also lead to inconsistencies.

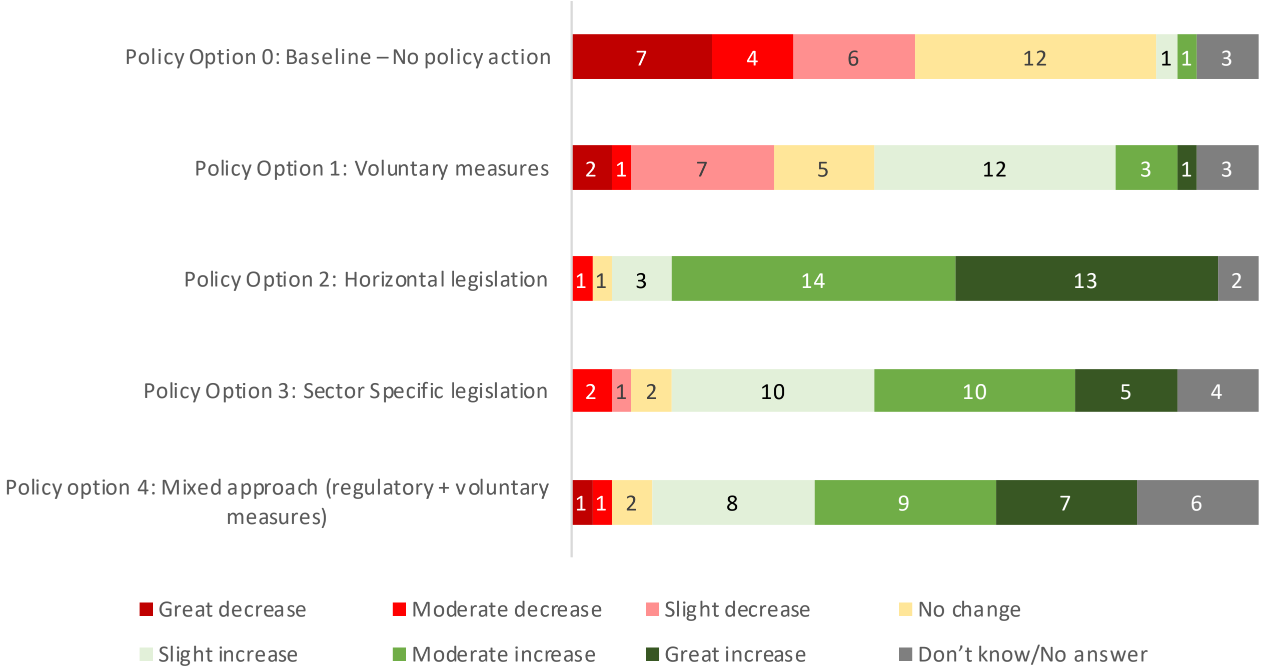
However, alternative views also emerged. A few stakeholders suggested that in case of horizontal legislation, regardless of the measures included in this regulatory framework, some manufacturers may consider not profitable to take their products to the EU market. The GDPR experience suggests this is plausible considering there are web sites that have left the EU market as a consequence of the new GDPR regulation. Because the nature of the measures is unknown at the moment, it is only reasonable to assume that a moderate number of manufacturers will not take their product to the EU market as a result. The magnitude of the impact will depend on the measures included in the Horizontal legislation.

During the **Targeted Consultation**, horizontal legislation was much more frequently deemed as having a significantly positive impact on the availability of reliable and secure ICT products in the Internal Market compared to the other policy options. Only 35% of the respondents deemed sector-specific legislation would have a significantly positive impact in this regard while 41% of the respondents thought the same about the mixed approach. The most frequent comment related to the benefits of introducing horizontal legislation which would cover most ICT products with sufficiently high and uniform security standards. One NCA also added that independent conformity assessments under CSA would grant reliable and secure ICT products compare to voluntary measures.

Impact on the trust in ICT products and the Digital Single Market

Concerning the impact on the **trust in ICT products and the Digital Single Market**, in line with the previous question on reliability and security, stakeholders believe Horizontal legislation would be the most impactful (positive) on trust, followed by a Mixed approach and Sector-specific legislation (Figure 51). Voluntary measures might result in slight increase while No policy action is likely to have no change or even decrease trust.

Figure 51 Impact on the trust in ICT products and the Digital Single Market



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

Stakeholders mentioned that without any regulatory measures in place, consumers will most likely perceive a fragmentation in the standards of cybersecurity of ICT products and insufficient consideration of such standards. The current level of cybersecurity in ICT products is not regarded as satisfactory or mature enough -especially in a B2C context. The situation will likely worsen if no action is taken. Voluntary measures might lead to a weak impact because only companies with already high security standards will provide such voluntary measures. This might also contribute to higher concentration in the market.

The impact (positive) on trust would increase the most in a mandatory horizontal regulation scenario because all products would fulfil the security requirements, hence, achieving a level-playing field. However, if requirements were implemented inconsistently or overlapping, the situation would deteriorate due to the accrue complexity, conflicting effects on stakeholders and misleading responsibilities. Thus, only a horizontal approach was regarded to strengthen cybersecurity with more certainty.

Stakeholders highlighted that the issue of trust in ICT products is convoluted in two main drivers, namely, an increasing need to manufacture more complex ICT products and systems and buyers being unable to check products. The first factor highlights the fast pace of technological change and the market pressure to innovate which may be at odds with cybersecurity to some extent, while the second factor represents an issue of asymmetric information (i.e. a market failure). Such market dynamics on the supply and demand side may lead innovators to buy tools and elements that result in sub-optimal levels of cybersecurity. Stakeholders showed some concern towards the level of cybersecurity in ICT products in a context without proper rules because consumers still need to buy such products but without necessarily trusting the level of security. In other words, the market will not adjust automatically or exclude ICT products from the market. Therefore, stakeholders stressed the need to put in place regulation that makes manufacturers accountable for the level of cybersecurity in their ICT products.

During the **Targeted Consultation**, horizontal legislation was deemed by the majority of the respondents (51%) to be most likely to generate a significantly positive impact regarding trust in ICT products compared to the other policy options, even if 47% and 44% of the respondents thought that the sector-specific legislation and the mixed approach would respectively have a significantly positive impact on trust in ICT products.

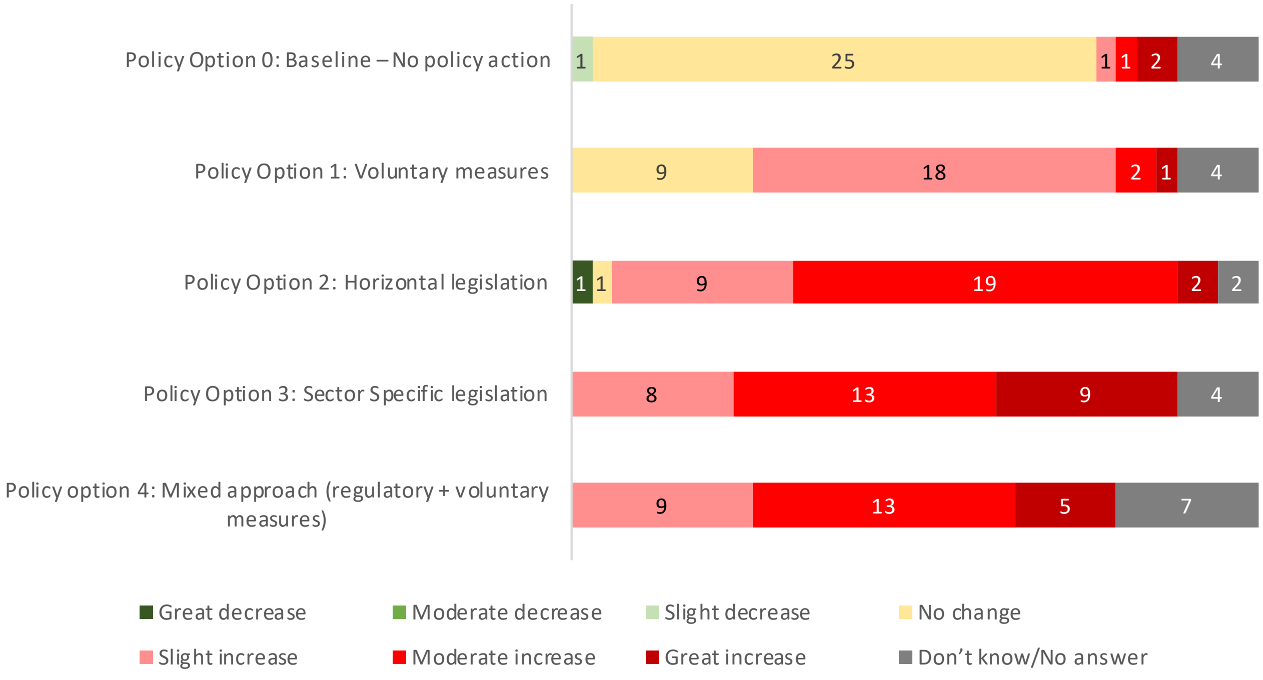
6.2 Efficiency and economic impacts

This Section delves into the likely impacts on costs stemming from policy option as perceived by stakeholders. In addition to this primary data collection, the Project Team has conducted a desk research to map potential impacts of the policy options. The evidence reviewed so far points to different approaches to cost security measures. For example, a systematic review mapping the relationship between security and software development found that the approaches to estimating costs are quite heterogenous and are not empirically validated. The lack of empirical validation means these approaches are not adopted and hence do not produce historical data. The range of estimated values varies remarkably[349]. In another study, a survey on the application of software security practices aimed to identify the impact of enhancing security in software development projects. The findings highlight that security measures were applied thoroughly in the projects, showing high variability in secure software development effort. Respondents manifested that security is key driver for the effort in software and security measures must be considered when planning software development interventions[350]. A study exploring the software security investment modelling highlighted that there is limited available evidence on software security investment due to its recent area of focus [351]. These studies confirm the difficulties the Project Team has encountered in finding cost data related to cybersecurity of ICT products from secondary sources. Therefore, the remaining of this Section relies on primary data.

Overall impact of policy options on costs based on stakeholder consultation

When asked about the **potential costs of each policy option**, stakeholders agreed that the baseline option would present no change, as expected (as presented in Figure 52). Horizontal legislation was considered the most expensive followed by Sector-specific legislation and a Mixed approach.

Figure 52 Impact on costs of each policy option



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

[349] Elaine Venson, Xiaomeng Guo, Zidi Yan, and Barry Boehm. 2019. Costing Secure Software Development – A Systematic Mapping Study. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom. ACM, NewYork,NY, USA, 11 pages. https://doi.org/10.1145/3339252.3339263

[350] Elaine Venson, Reem Alfayez, Marilia M. F. Gomes, Rejane M. C. Figueiredo, Barry Boehm. 2019. The Impact of Software Security Practices on Development Effort: An Initial Survey. Authorized licensed use limited to: European Commission - Joint Research Centre_Italy. Downloaded on April 07, 2021 at 12:44:45 UTC from IEEE Xplore.

[351] Heitzenrater, C.D., 2017. Software security investment modelling for decision-support (Doctoral dissertation, University of Oxford).

When prompted to elaborate on their answers…

Most respondents highlighted that **the no policy action scenario will have no significant costs in the present**. A few stakeholders mentioned the importance to assess the need to secure the equipment used in Europe. However, it was manifested that a business-as-usual scenario would lead to a great increase in costs in the medium and long term. Hence, the timing of costs (short, medium and long term) makes a significant difference for the appraisal.

Voluntary measures were perceived by several stakeholders as being as impactful as the baseline option, that is, overall limited. However, they also noted that horizontal or sector-specific legislation are likely to be more burdensome to SMEs than larger companies. Voluntary measures, complemented by a reviewed NIS Directive, was considered a good approach as it would combine voluntary measures with legislative provisions that will address security requirements for all ICT products. Stakeholders highlighted that software and hardware providers should be recognised as essential entities under the NIS Directive.

On horizontal legislation, few stakeholders highlighted a "moderate increase" assuming that horizontal legislation will apply across all ICT products. The magnitude of the increase will depend on the measures included in the legislation. That being said, horizontal legislation is a blanket instrument that will require a trade-off in regard to the kinds of risks it will address. Some stakeholders suggested that if the service were widely deployed, costs would not increase significantly. Better product security would be balanced by lower maintenance. If horizontal standards are adopted for all products, procedures will evolve, software modules will implement these standards and the real impact on costs will soon diminish. The biggest cost would be a set-up cost at the start, to change procedures and update software. Costs are likely to drop after the initial remastering.

On the other hand, it is argued that some horizontal legislation would unavoidably be too rigorous for some sectors and products and thus have a significant effect on cost. Also, it is argued that horizontal or sector-specific legislation implemented without clear guidance but including high fines can be very costly.

On sector-specific legislation, some stakeholders expressed difficulty to estimate costs without precise information on the sectors affected. Other stakeholders foresaw considerable costs due to multiple and potentially overlapping requirements which need to be checked for consistency.

Likewise, on a mixed approach, stakeholders expressed difficulty to estimate costs without exact detail on the ICT products under scope.

During the **Targeted Consultation,** respondents most frequently indicated that No policy action would result in a small increase in costs generally, especially compliance costs for ICT businesses (60% of all respondents).

The introduction of horizontal legislation would result in a small cost increase overall compared to No policy action: 51% of the respondents indicated that compliance costs for ICT businesses would slightly increase while a further 28% indicated that these would increase significantly. In addition, 48% of the respondents indicated that monitoring and enforcement costs for NCAs would increase slightly while a further 31% indicated that these would increase significantly.

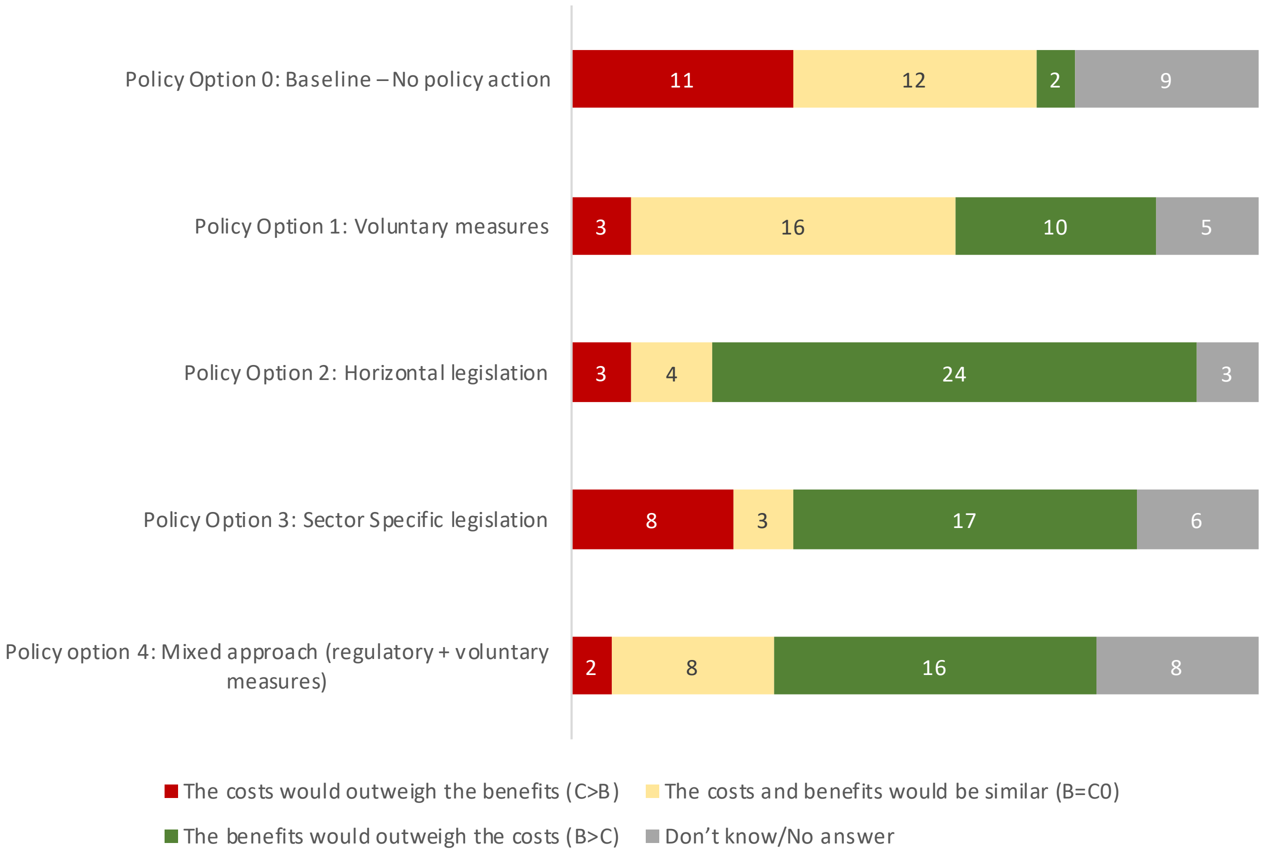
Respondents indicated overall that the introduction of sector-specific legislation would result in small to significant cost increases overall compared to no policy action: 53% of the respondents indicated that the administrative burden for public authorities would slightly increase while a further 26% indicated that these would increase significantly. In addition, 45% of the respondents indicated that compliance costs for ICT businesses would increase significantly while a further 31% indicated that these would increase slightly. Interestingly, 40% of the respondents indicated that policy option 3 would mean slightly higher prices for consumers with a further 16% indicated this would result in significantly higher consumer prices.

The mixed approach was deemed as resulting in small to significant cost increases compared to no policy action, but to an even greater extent than the sector-specific legislation. For 47% of the respondents, monitoring and enforcement costs for NCAs would increase slightly while these would increase significantly for a further 31%. Similarly, 47% of the respondents indicated that the administrative burden for public authorities would increase slightly with a further 28% indicating these would increase significantly. Most respondents (77%) also deemed that the mixed approach would increase compliance costs for ICT businesses either slightly or significantly.

Impact of policy options on the cost-effectiveness

Interestingly, **stakeholders ranked horizontal legislation first for the cost-effectiveness** (as described in Figure 53). This was followed by sector-specific legislation and a mixed approach. Stakeholders' views seem to diverge on the cost-effectiveness of the sector-specific legislation. For example, 17 out of 34 believe the benefits would outweigh the costs whereas 8 believe the opposite[352].

Figure 53 Cost-effectiveness of the policy options



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

[352] 6 out of 34 didn't know and 3 considered benefits would equal costs

When prompted to elaborate on their answers…

On voluntary measures, its impact would depend on the responsiveness of demand for product differentiation. Consumers that buy into higher cybersecurity standards are likely to encourage companies in adopting such voluntary measures, as it would mean their products sell more. Stakeholders noted that there can be a significant cost attached to “doing nothing or very little”. This stems largely from increased cybersecurity incidents and a loss of trust in digital transactions. The lack of action would not be free of cost for consumers and the loses due to lack of security in ICT products is likely to increase.

One issue with **horizontal legislation** is that it would not be adapted to each market. As markets are different, adapting regulatory requirements according to sectors according to minimum security levels is a good way to differentiate costs, and therefore reduce them overall. Horizontal legislation can be a “blunt tool”. However, another respondent claims, a horizontal legislation is likely to have a much larger impact on cybersecurity levels than a fractured approach. A universal approach will also improve regulatory clarity, allowing for the simplification of administrative procedures. Overall, most respondents consider this to be the most cost-effective approach.

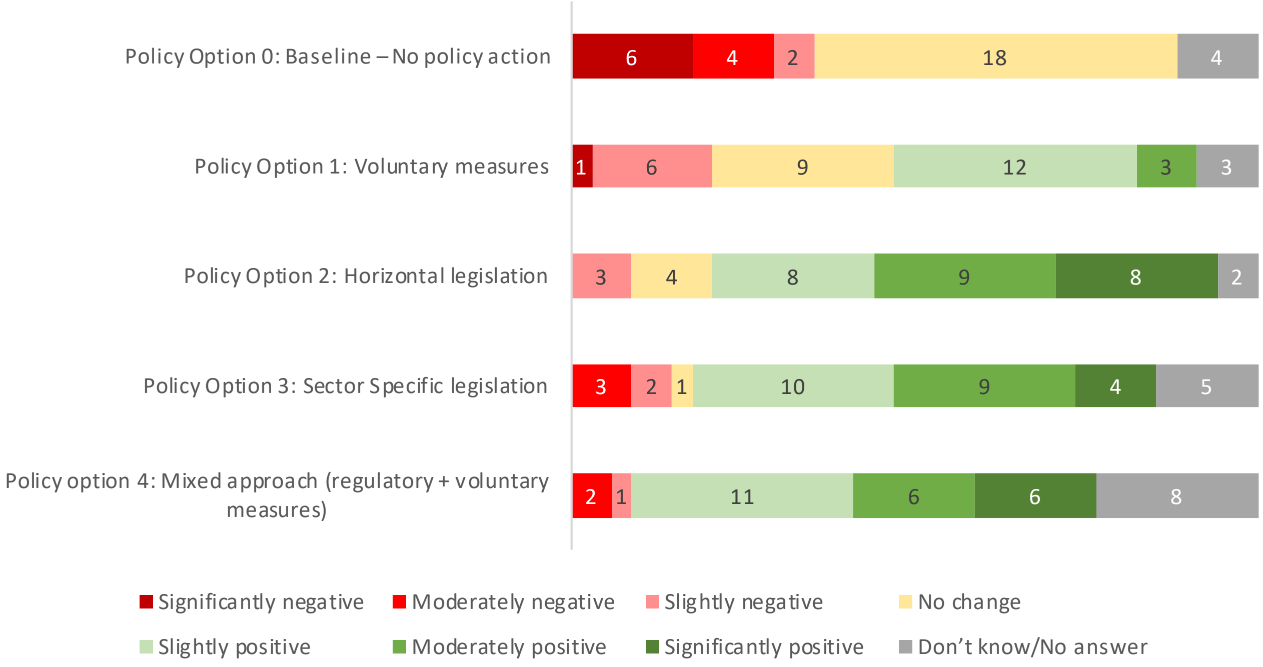
On Sector-specific legislation, a more complex system of conformity assessment is likely to push costs up. Another respondent reports that a more focused policy may have higher initial costs, but a smaller burden in the long term. However, these initial costs are emphasised by multiple respondents, defending that a fractured approach is likely to lead to doubling of efforts.

During the **Targeted Consultation**, horizontal legislation was deemed to be cost-effective by 58% of the respondents while sector-specific legislation was deemed to be cost-effective by 52% of the respondents and the mixed approach by 50% of the respondents. Respondents were most likely to indicate that the costs of voluntary measures would outweigh its benefits. A few respondents made comments on cost-effectiveness, the most frequent ones suggested horizontal legislation to be the most cost-effective.

Impact on the competitiveness of the ICT industry

Looking at the **overall impact on the competitiveness of the ICT industry**, the horizontal legislation is the most popular. This is followed by sector-specific legislation, with a Mixed approach coming in third place. Interestingly, the business-as-usual option is expected to have a negative impact on the competitiveness of the ICT sector.

Figure 54 Impact of the policy options on the competitiveness of ICT industry



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

Some respondents believed the proposed policy options could not significantly alter the competitiveness of industry. They argue that change has to come from the demand side, from a preference for more secure products. Arguably, any improvement in product security could improve the competitiveness of ICT products internationally. Trust is an important factor in competitiveness, and branding ICT products as "certified in EU" could bring the extra value to EU Digital Single Market and leverage on the global market.

Some respondents supported **horizontal legislation** assuming that this would set an even playing field across companies and encourage competition. A horizontal measure would ensure all manufacturers – both within and outside the EU – follow the same rules. It would work by raising the standards bar while avoiding large market distortions. From that raised bar, manufacturers would be able to increase their competitiveness by creating more secure products. However, horizontal legislation may impose disproportionate costs to some sectors, affecting their competitiveness internationally.

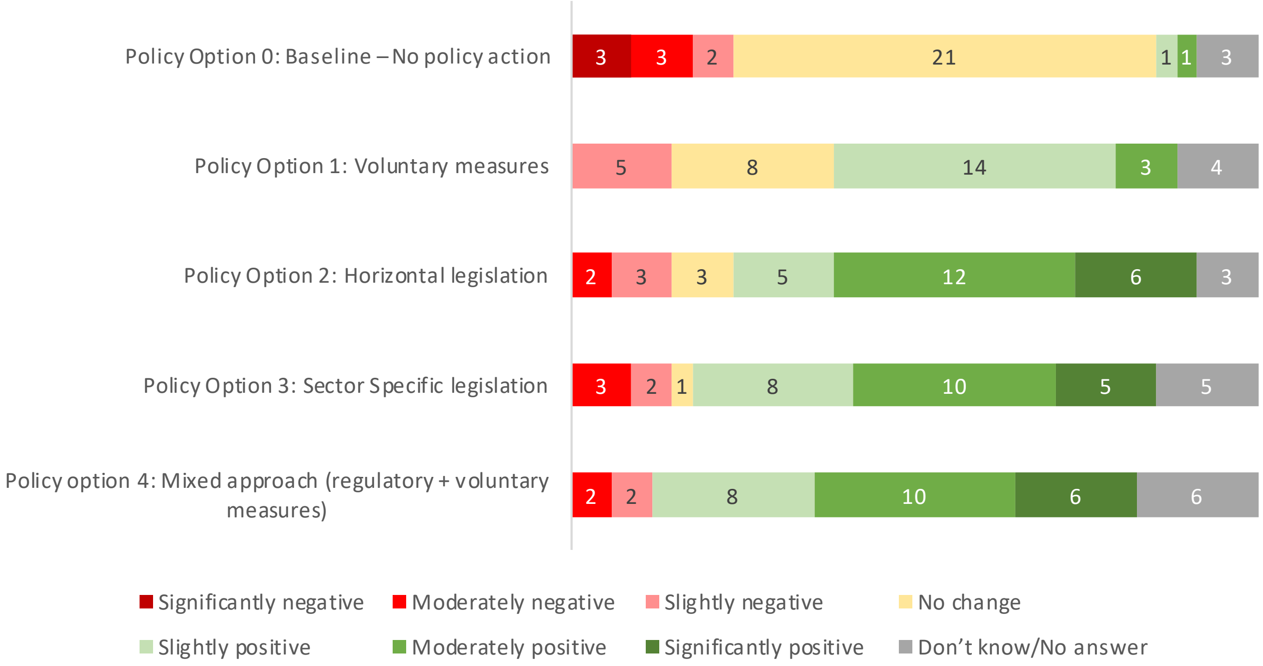
A **mixed approach** would combine the benefits of a targeted legislation with those of voluntary measures, a few stakeholders argued.

During **the Targeted Consultation**, of all the policy options, horizontal legislation was most frequently deemed to be likely to generate significantly positive impacts on the competitiveness of the EU's ICT industry (33% of all respondents), followed by mixed approach (30% of all respondents). Sector-specific legislation was most frequently deemed likely to generate moderately positive impact on the competitiveness of the EU's ICT industry (51% of all respondents).

Impacts on the innovation in the ICT industry

In terms of the effect of policy options on **innovation in the ICT industry**, horizontal legislation comes out on top. A Horizontal legislation maybe interpreted by some as maintaining an even playing field among different companies. The second most beneficial policy in encouraging innovation would be a mixed approach, closely followed by sector-specific legislation. It is interesting to note on that industry stakeholders are divided on the impact of horizontal legislation. Two believe that the impact on innovation will be "moderately negative", whereas three report it will be "significantly positive".

Figure 55 Impact of the policy options on the innovation in ICT industry



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

Some respondents claimed that **horizontal legislation**, being a blanket measure, can have a detrimental effect on innovation within the ICT industry. However, such regulatory approach may encourage sharing of information and best-practices across companies and sectors, encouraging innovation in those least advanced sectors.

When considering innovation in the economy as a whole, higher level of cybersecurity is expected to be positively associated with innovation in the digital landscape, as the risk of cyberthreats should fall. Stakeholders recommend an evaluation against related legislation such as the RED and Cybersecurity Act.

Voluntary measures would treat higher cybersecurity standards as a competitive advantage. If there is a positive response from the demand side this could lead to significant incentives for innovation.

Horizontal legislation is believed to foster the development of best practices and building blocks which can be reused for a wide variety of product categories, a respondent argues. Mandatory security measures are thought to encourage innovation and standard setting in the long term, an example being the car industry. However, it is unlikely that universal measures applicable to all sectors will be at the cutting-edge of cybersecurity. This is because costs will have to be balanced out for sectors less affected by cybersecurity threats. It is also noted that requirements under a horizontal legislation have to be flexible enough to allow for new innovative ways to raise cybersecurity. This would mean norms and standards are preferred to technical requirements, as they can respond better in a fast-changing threat environment.

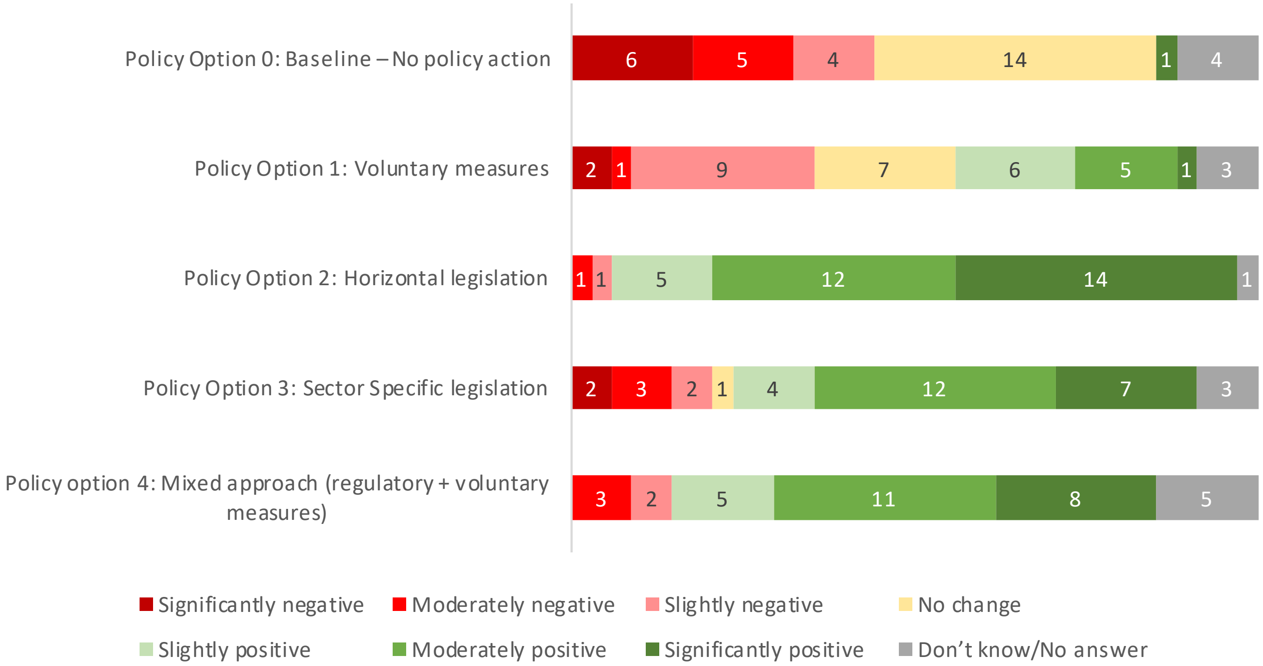
Some respondents expected that **sector specific legislation** would lead to excessive administrative burdens, hindering innovation. However, strict regulations could provoke researchers to find optimized solutions, whereas with no regulations they tend to provide trivial solutions, argues a second respondent.

During **the Targeted Consultation**, of all the policy options, horizontal legislation was most frequently deemed to be likely to generate significantly positive impacts on innovation in the EU's ICT industry (20% of all respondents). Sector-specific legislation was most frequently deemed likely to generate moderately positive impact on the innovation of the EU's ICT industry (41% of all respondents).

Impact of different policy options on the functioning and harmonisation of the Internal Market

On the impact of different policy options on the **functioning and harmonisation of the Internal Market**, the results point to a horizontal legislation. Many respondents expect voluntary measures to have a negative impact on the harmonisation of the internal market. Sector-specific legislation and a mixed approach are also expected to have a positive impact.

Figure 56 Impact of the policy options on the functioning and harmonisation of the Internal Market



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

Respondents support that any legislative measures introduced in the EU level would have a positive impact on harmonisation of Internal Market. An absence of common rules may produce incompatible systems and offers in the ICT sector. Nevertheless, Member States should not be prevented from adopting their own higher-level requirements on high-risk products.

Taking **no action** is expected to negatively impact the harmonisation of the internal market in the long run. This will happen as countries start taking regulatory initiatives at different times and with a varying level of commitment.

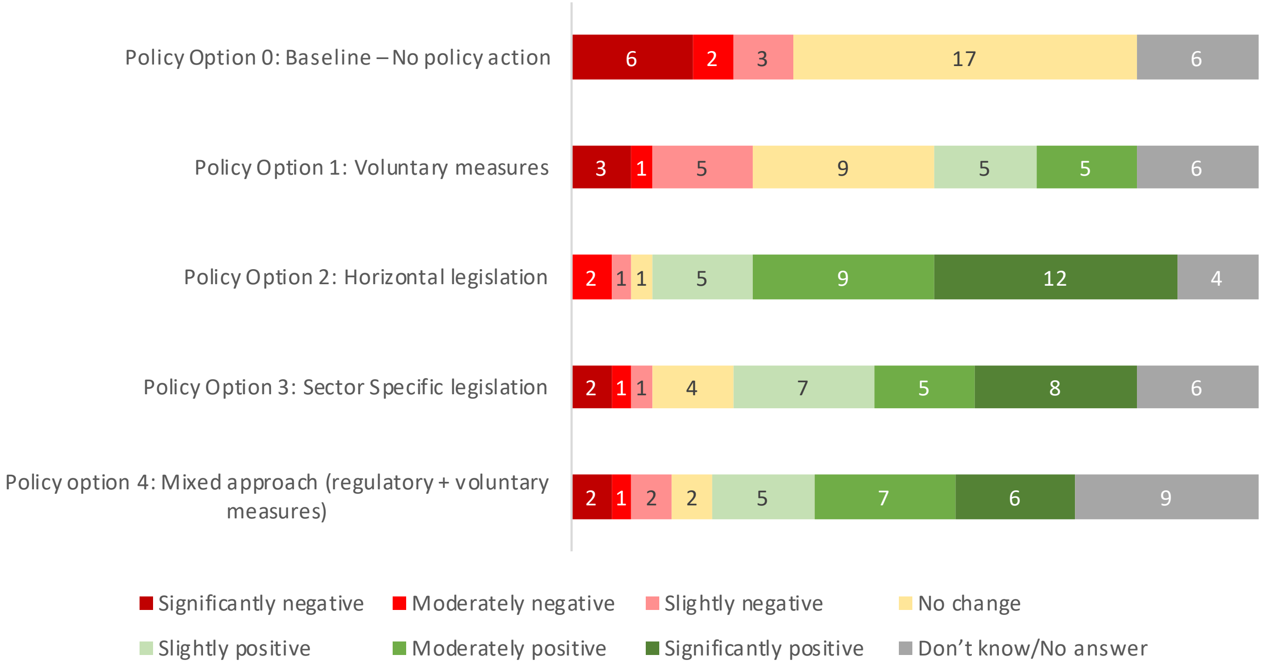
Horizontal legislation is believed to avoid market fragmentation, and therefore promote the harmonisation of the Internal Market. The market will benefit if all know and abide by the same rules. However, horizontal legislation requires a trade-off between coverage and risks addressed. Essential requirements are often too high level and pose difficulties to develop harmonized standards that can be used for product assessment. It is argued that more specific requirements should be defined on top of a baseline.

It is more difficult for respondents to assess **sector-specific legislation** or a **mixed approach** without further information on the ICT products to be affected. It is mentioned that these should be avoided in terms of achieving greater internal market harmonisation. This is because sectors have different needs between countries. Nevertheless, the argument for sector-specific legislation is that a horizontal legislation may cause a reaction against overregulation.

Impact on fair competition

Regarding the impact on **fair competition**, the clear favourite is horizontal legislation (as described in Figure 57). The argument is to avoid the creation of different legislation across countries. If this were to happen, it would be more harmful for businesses operating across EU borders. A sector-specific legislation and a mixed approach are also expected to have a positive impact on creating a level playing field for the ICT product market. There are no respondents that believe the baseline scenario could have a positive impact on fair competition.

Figure 57 Impact of the policy options on fairness in competition in the Internal Market



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

Respondents expressed similar view to the question on harmonisation of the internal market. It is reiterated that Member States should not be prevented from adopting their own higher-level requirements on high-risk products.

Taking **no action** will lead to each Member State addressing the issue individually, creating a fragmented market overall.

As the answers reflect, most respondents believe that **horizontal legislation** achieves a level playing field on the internal market. It is assumed consumers are more elastic to price changes than changes in technical elements of ICT products. Therefore, any differentiation between countries or sectors will create an unfair advantage for those unaffected by regulation. Also, pan-European standards may benefit European exports in international markets. This is likely to have a larger impact on exporting Member States with an advanced ICT sector, such as Germany. Nevertheless, other respondents argued that a risk-based approach for security evaluation should be encouraged, in which manufacturers can demonstrate the security level of its connected devices without being constrained by rigid criteria.

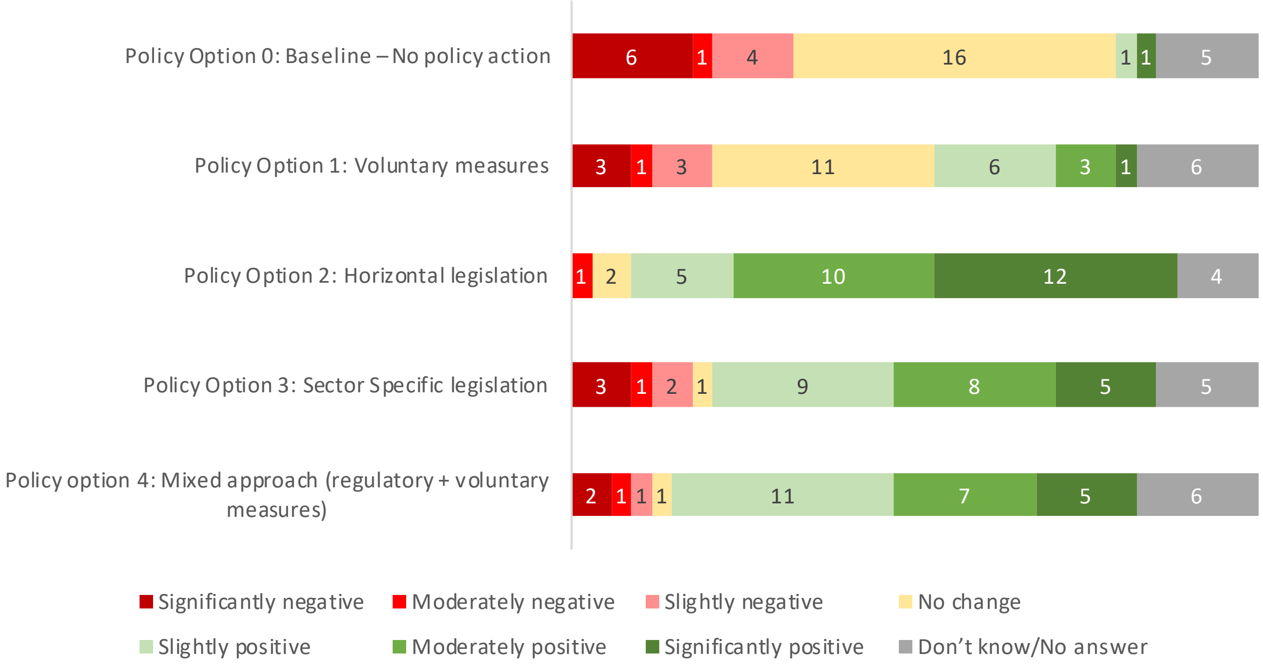
A **sector-specific** legislation could be beneficial. It is argued that imposing costs on products or sectors where they are not appropriate is not fair. This could limit the international competitiveness of such over-regulated products or sectors.

During **the Targeted Consultation**, horizontal legislation was much more frequently deemed as having a significantly positive impact on creating a level-playing field in the EU ICT market (40% of all respondents) compared to the other policy options. Only 26% of the respondents deemed sector-specific legislation would have a significantly positive impact on the EU ICT market and only 24% of the respondents thought the same about the mixed approach.

Impact on the Digital Single Market

Finally, when asked about the impact of the policy options on **stimulating the Digital Single Market**, most respondents predict that horizontal legislation would be most beneficial. Similar to previous responses, sector-specific legislation and a mixed approach rank in second place. No respondents believe that taking no action can stimulate the Digital Single Market, and they are divided about the potential impact of adopting voluntary measures. Interestingly, competent authorities tend to believe that voluntary measures could have a positive effect, whereas academic experts support the opposite side.

Figure 58 Impact of the policy options on stimulating the development of the Digital Single Market



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

When prompted to elaborate on their answers…

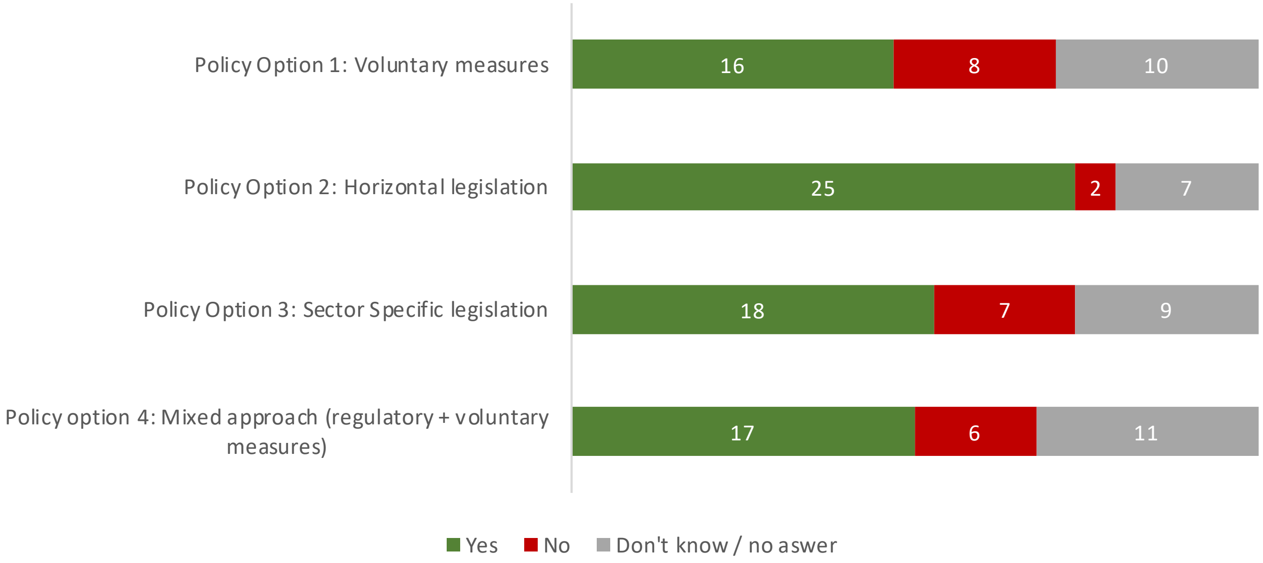
Some respondents argued that **voluntary measures** are likely to cause fragmentation between countries. Producers in Member States which are at a later stage of digitisation may adopt voluntary measures more readily, leaving some countries more exposed to cyberattacks.

Other respondents thought that **horizontal measures** can avoid sectoral and national fragmentation. On one hand, guaranteeing a certain level of cybersecurity can promote new digital products and services. Also, adhering to certain uniform standards can make European exports more attractive abroad. On the other hand, horizontal measures can lead to a compromise in cost and efficacy for those products, which may start a race to the bottom for the overall level of cybersecurity across the value chain.

6.3 Coherence

Stakeholders thought that all policy options were potentially coherent with other EU and national initiatives (Figure 59). Most of them supported Horizontal legislation. According to some stakeholders, only Horizontal legislation would lead to a fully coherent state of play. Other policy options were regarded as contributing to coherence at least in theoretical term but experience suggest this may not be attained. Both sector-specific legislation and mixed approach risk regulatory fragmentation, which may place in difficulty producers/operators of ICT products and services. It was highlighted that coherence does not depend on the regulatory framework per se but how policy options are implemented. For example, a future legislation should be aligned to the NLF as established in 768/2008EG which was considered feasible if this is a NLF-regulation.

Figure 59 Coherence with other EU and national initiatives



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

During **the Targeted Consultation**, within the ICT industry players stakeholder group, the most frequent responses given were that horizontal legislation is the option that could make product policy coherent. Without such framing legislation, the other regulations risk to be incoherent or even contradictive. If horizontal legislation is introduced, there is no need to regulate on other initiatives. A horizontal law has the potential to yield more legal certainty and legal coherence in Europe. This would apply to all stakeholders along the value chain, which would increase the overall level of cybersecurity in the EU. The horizontal approach would make some initiatives currently under development, such as the RED delegated act, redundant since it can cover the same aspects more coherently as well as address a larger scope.

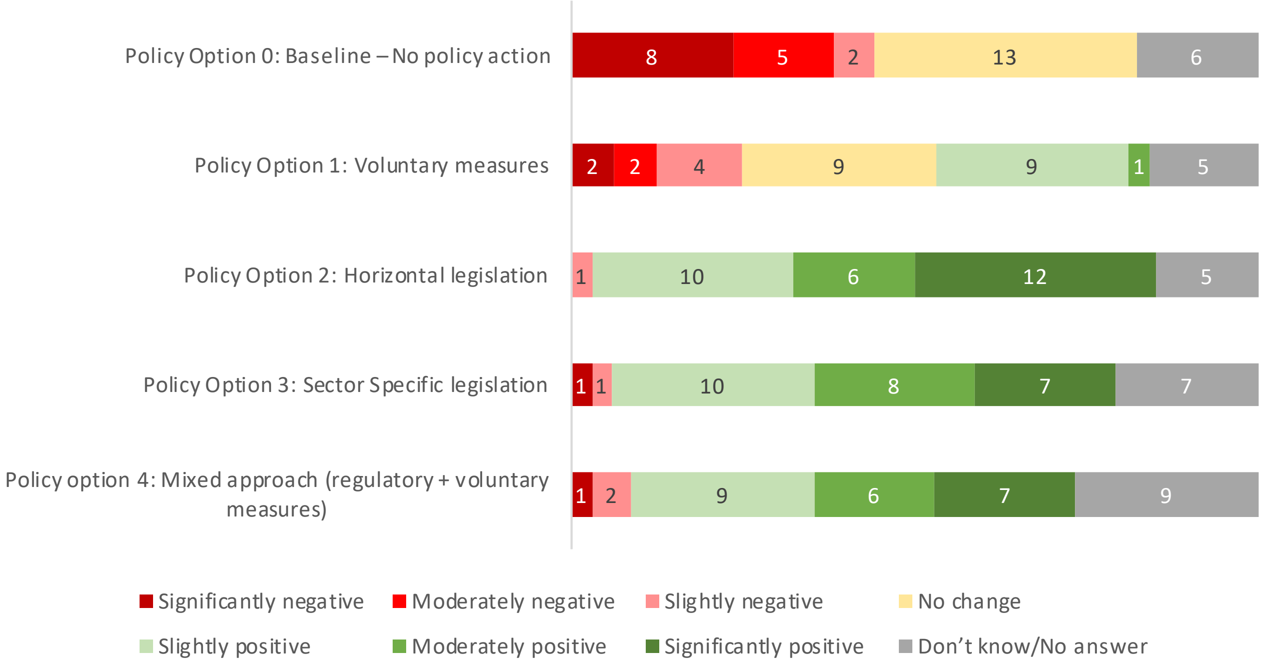
At the same time, among the other respondents on behalf of the ICT industry, eight argued that horizontal legislation could also potentially lead to incoherence with other EU initiatives. Specific concerns include the possibility for overlap with other legislation, discrepancies could arise within specific sectors and/or national implementations, and that horizontal legislation may conflict with CSA, NIS and NLF regulation.

Six respondents on behalf of NCAs shared the view that introducing horizontal legislation could lead to duplications in an effort to ensure sufficient specificity through *lex specialis* clauses. However, seven respondents on behalf of NCAs believe that whilst there could be coherence issues these could be mitigated by careful formulation or amendment of other relevant legislative acts.

6.4 Fundamental rights

The most positive impact on fundamental rights (i.e. protection of personal data, consumer protection, protection of liberty and security) is expected from Horizontal legislation, closely followed by sector-specific legislation and Mixed approach (Figure 60). Voluntary measures are expected to have slight positive change or none, while a No policy action would have a negative impact.

Figure 60 Impact on fundamental rights



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

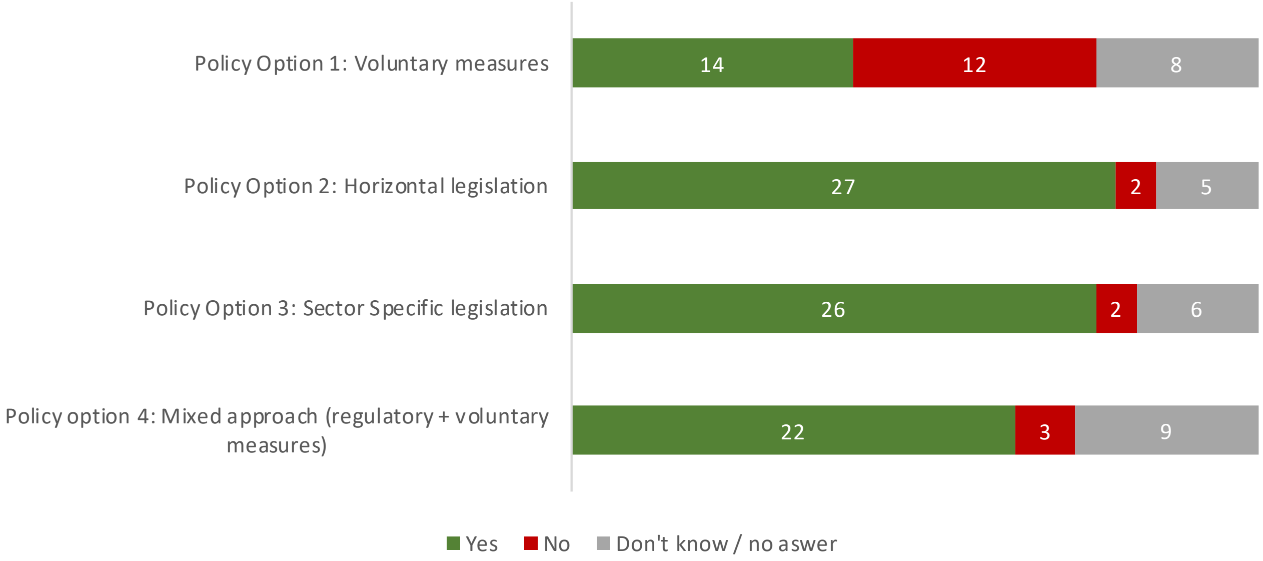
Stakeholders thought that consumers can be best protected with the help of a policy option that covers all types of products. Therefore, horizontal NLF-based approach would ensure that the CE marking does not only stand for safety but also for a product's cybersecurity. At the same time, a higher level of cybersecurity would have beneficial societal impacts, but the trade-offs also should be considered. At some point, requirements could be too high for too little reward, especially if they cut deep into the freedoms of economic operators. Stakeholders manifested that it might take some time and adjustments to find a right level of adequate cybersecurity. Therefore, it is especially important to choose the most effective, efficient and consistent way to address this problem.

During **the Targeted Consultation**, horizontal legislation was most frequently identified as the most effective and efficient in generating positive impact on fundamental rights, especially among respondents on behalf of the ICT industry. A few comments were received on the policy options' potential impact on fundamental rights. One respondent on behalf of the ICT industry commented that the most effective approach would combine a horizontal baseline of security requirements with different specific requirements for each vertical sectors. It was remarked by three respondents that although consumer protection is a fundamental right and cybersecurity is only indirectly related, a regulation on ICT product security can be expected to impact fundamental rights positively. One respondent on behalf of a European institution pointed out that while fundamental rights are already covered by the GDPR, the ICT industry would benefit from clear regulation and technical guidelines that would improve compliance with the GDPR.

6.5 EU added value

Except for Voluntary measures, all other policy options are expected to add EU value compared to Member States acting separately (Figure 61).

Figure 61 EU added value of the policy options



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

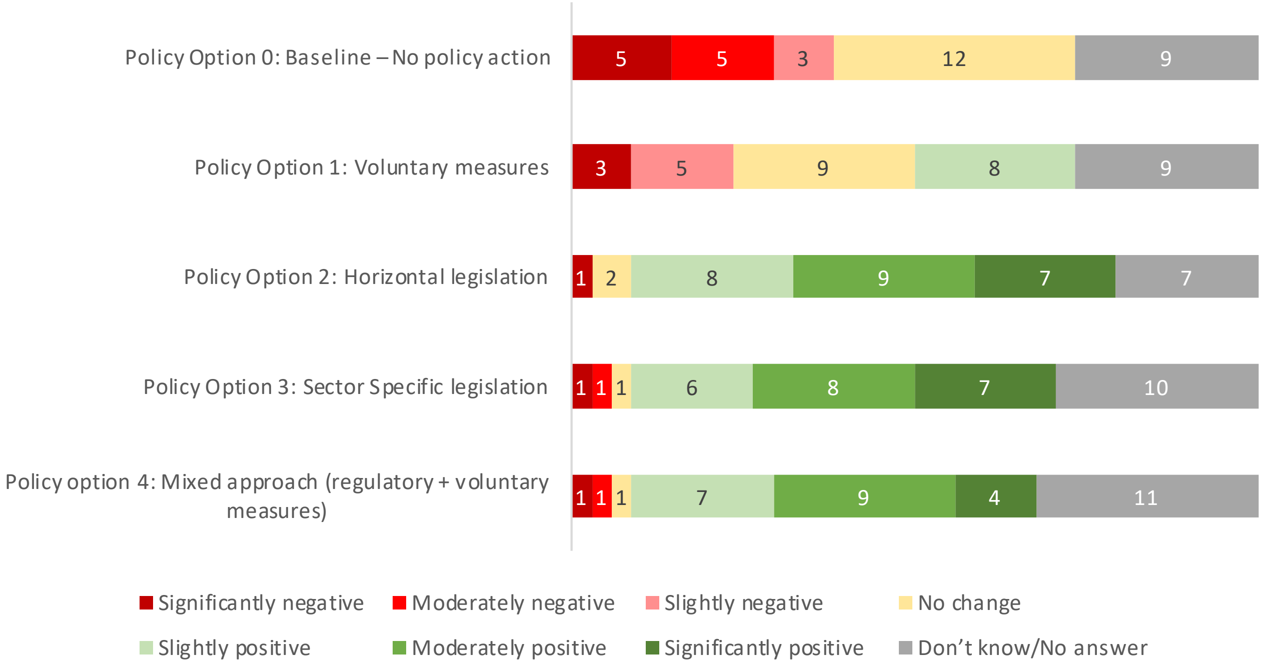
During **the Targeted Consultation**, horizontal legislation was the only of the four to be deemed by the majority of the respondents (52%) as generating significant EU added value compared to Member States acting separately. Overall, 86% of the respondents agreed that horizontal legislation would generate EU added value. By comparison, three quarters of the respondents agreed that the sector-specific legislation and the mixed approach added value (76% and 75% respectively). Only 41% of the respondents agreed that voluntary measures would generate EU added value.

A few respondents commented on the potential EU added value of each of the four proposed policy option. Across all stakeholder groups, but particularly among respondents on behalf of the ICT industry and professional users, the most frequent comment was that the introduction of horizontal legislation would generate the greatest EU added value as it would prevent market fragmentation and the emergence of Member State-specific laws on ICT product security; in other words, horizontal legislation is considered as having the highest potential in contributing to the consolidation of the European Digital Single Market.

6.6 Environmental impact

Horizontal legislation, sector-specific legislation and Mixed approach are likely to have positive impact on the environment (see Figure 62). Voluntary measures are expected to have no change and No policy action might lead to negative impact on the environment. Stakeholders thought that with systems being ever closely connected, the risk of environmental damage due to cyber incidents will increase over time. Thus, legislation is preferred. The policy options including horizontal component should most effectively protect the environment as a natural consequence of driving up safety and security.

Figure 62 Impact on the environment



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

6.7 Comparative assessment

This Section aims to summarise the qualitative and quantitative estimates. The qualitative assessment is done through a scoring system as described in Table 73. with symbols which have a numerical meaning only for the final scoring of policy options.

Qualitative assessment

The policy options are assessed qualitatively following the framework presented in Table 73.

Table 73 Scoring system for the qualitative assessment

Score	Numerical score	Impact level
+++	3	Highly positive
++	2	Moderate positive
+	1	Small positive
≈	0	Negligible effect
-	-1	Small negative
--	-2	Moderate negative
---	-3	Highly negative
?	n/a	Uncertain or lack of evidence to assess

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Quantitative assessment

Costs of policy measures

To assess potential costs of policy measures, the Project Team used as benchmarks the results from the Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment[353], a study on Evidencing The Cost Of The UK Government's Proposed Regulatory Interventions For Consumer IoT[354], and interviews conducted as part of this study. The Project Team asked Delphi respondents to assess whether the costs calculated in the studies would be higher, the same or lower in the context of the Cybersecurity of ICT products.

Self-assessment costs

The Radio Equipment Directive (RED) IA study estimated that self-assessment would demand two FTE months for an average firm, which translates to EUR 18 400 in staff costs (hourly rate ≈ EUR 29). Stakeholders were asked whether they envisage a lower/same/higher cost and or FTE in the context of cybersecurity of ICT products. Stakeholders thought they might potentially be **higher than EUR 18 400** (Figure 63). It would also heavily **depend on the type of product, the number of models, the uptake of the new models, the size of the organisation and finally on the specific requirements**.

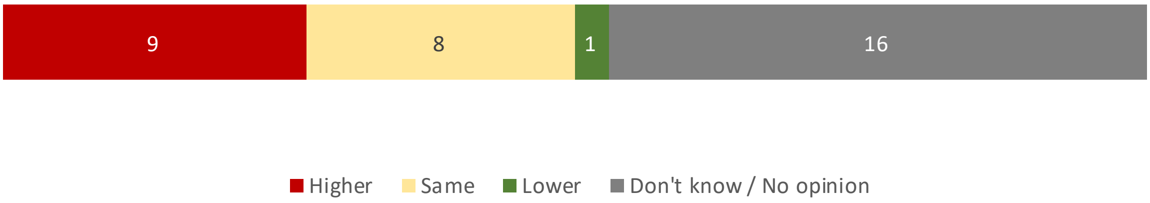
Conformity assessment under the RED is based on tests free of subjective criteria (i.e. tests of a "Pass"/"Fail" nature). The assessment of cybersecurity protection requires an assessment of the risks. The latter includes the asset, its operational context, and the capabilities of adversaries. All these assessments come with subjective factors. This means that **the current approach to legal certainty cannot be guaranteed when conformity assessments**

[353] The study is available at: https://ec.europa.eu/docsroom/documents/40763

[354] The study is available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf

address cybersecurity. If cybersecurity is to be duly assessed in accordance to the RED, if that is at all possible in the current framework, it is certain that the costs associated with conformity assessments will increase.

Figure 63 Self-assessment costs in comparison to RED IA



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

Third-party conformity assessment costs

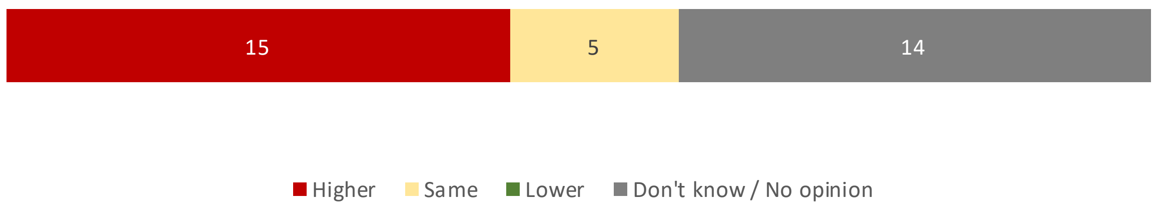
The RED IA study estimated the costs of third-party conformity assessment to be around EUR 2000-5000. Stakeholders were asked whether they envisage a lower/same/higher cost in the context of cybersecurity of ICT products. Most stakeholders thought the costs of third-party conformity assessment would be **higher than EUR 5000** (Figure 64). Without a detailed knowledge of essential requirements of the future legislation, they found it hard to estimate the expected costs. However, the more complex and demanding on the notified body the assessment is, the higher costs are to be expected. Particularly, **the costs would be higher in the initial stages of the implementation of a new legislation**. Later, the costs could decrease in relation to increase of business competition.

It is expected that human involvement in tests with subjective factors will incur a significant cost increase. Depending on economies of scale, the cost may be in the 100% to 300% range for a private stakeholder and their readiness to support such a conformity assessment. This estimate is a best guess, considering that the framework of conformity assessments under the RED is not fit for cybersecurity and may thus require process re-engineering for all stakeholders. Moreover, it may end up that notified bodies are the only viable path to market placement, assuming that notified bodies will be willing to assume the liability.

The costs will significantly **depend also on the product under consideration**. Moreover, due to a **low number of cybersecurity experts in third-party organisations**, the costs might sky-rocket at first as supply and demand will not easily match, as someone conducting the conformity assessment of a non-connected product cannot conduct the conformity assessment for a connected device, as specific cyber-related know-how will be needed. The massive shortage of skilled IT professionals will aggravate the situation.

Several stakeholders thought that, depending on the work done (i.e., document review, functional tests, penetration tests) the costs could **range from EUR 15 000 to EUR 50 000**.

Figure 64 Third-party conformity assessment costs in comparison with RED IA



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

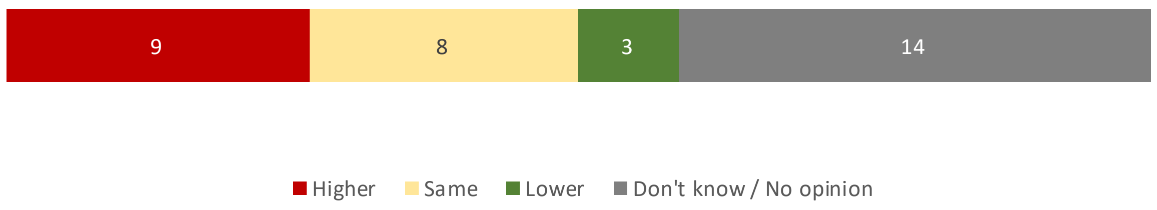
Testing costs of simple and complex products

The RED IA study estimated the costs of testing simple internet-connected products ranged between EUR 7 000 and EUR 15 000, and testing complex internet-connected products ranged between EUR 20,000 and EUR 30,000. Stakeholders were asked if they foresee a lower/same/higher figure in the context of cybersecurity of ICT products. Most stakeholders thought that the testing costs of simple products would be **higher than EUR 15,000** (Figure 65) while testing of complex products would be within **the range of EUR 20 000 and EUR 30 000** (Figure 66Without a detailed knowledge of essential requirements of the future legislation, it is hard to estimate the expected costs. However, stakeholders thought that the more complex and demanding testing is, the higher costs are to be expected. Particularly, the costs would be higher in the initial stages of the implementation of a new legislation. Later, the costs could decrease in relation to increase of business competition.

It will also depend on what are simple and what are complex products, and what would be “baseline” test (mentioned in the IA), which internal processes will be used. The figures are also difficult to estimate as the calculation of the in-house overhead is not straight forward.

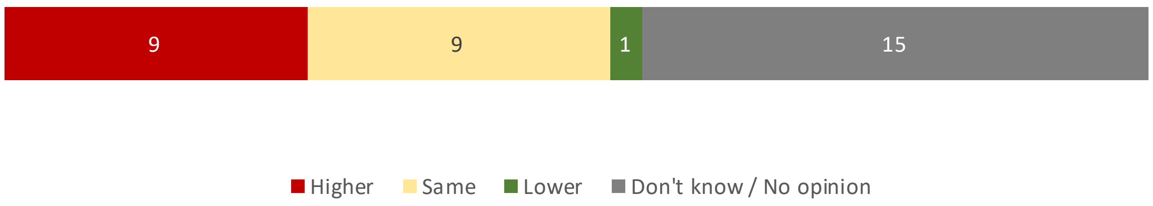
Interconnectedness increases the scope of the tests that will have to be done. Estimate is difficult, considering that the framework of conformity assessments under the RED is not fit for cybersecurity and may thus require process re-engineering for all stakeholder, Moreover, it may end up that notified bodies are the only viable path to market placement, assuming that notified bodies will be willing to assume the liability.

Figure 65 Costs of testing simple internet-connected products in comparison to RED IA



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

Figure 66 Costs of testing complex internet-connected products in comparison to RED IA



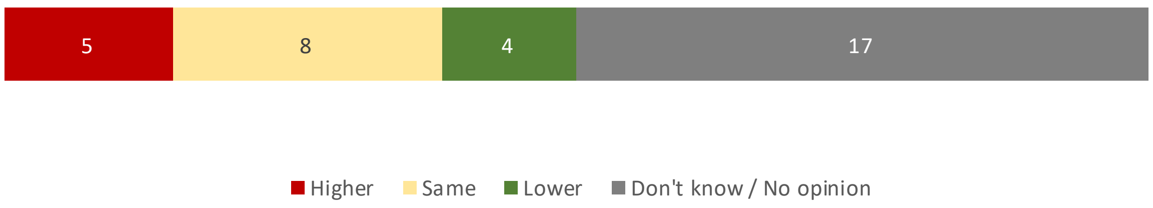
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

Cybersecurity label costs

Finnish vendors participating in the pilot of the Cybersecurity Label suggested the testing phase's costs range between EUR 10 000 and EUR 30 000. The duration of the inspection by a third party varies between approximately 5 and 20 working days. The cost per product of the inspection includes the right to use the label (EUR 350) and the annual review (EUR 350). Stakeholders were asked if they foresee a lower/same/higher figure in the context of cybersecurity of ICT products. Stakeholders thought that the costs of the **label's testing phase would be in the range between EUR 10,000 and EUR 30 000** and the costs of **inspection per product to be around EUR 700** (right to use + the annual review) (Figure 67). Without a detailed knowledge of requirements that would be tested, it is hard to estimate the figures. The cost might be higher because the assurances offered by the labelling scheme are relevant to a particular class of ICT products and do not address all the assurances levels that will apply for any ICT products.

The duration of the inspection is likely to increase if more product groups will have to be inspected, especially in light of a shortage of skilled IT personnel. Costs might also increase due to an increased demand for third-party inspections which – at least initially – will not be matched by a supply of skilled inspectors. It also depends on the depth of the testing and the complexity of the product.

Figure 67 Cybersecurity label costs in comparison to the Finnish pilot



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

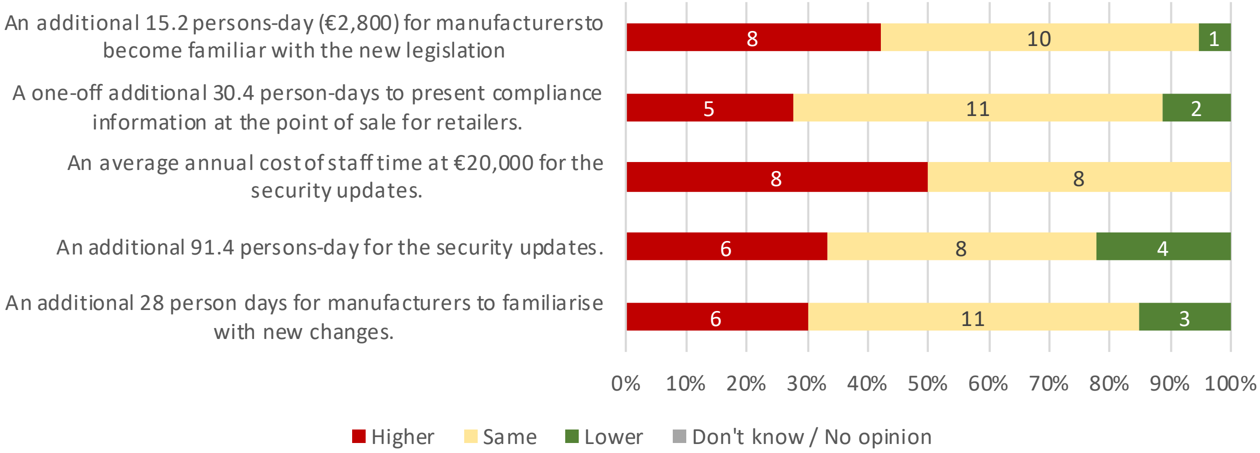
Code of conduct costs

In terms of codes of conduct, The UK code of Practice for Consumer IoT includes three security guidelines: default passwords, vulnerability disclosure and security updates. Stakeholders were asked if similar guidelines were introduced in the context of ICT products, do they foresee a lower/same/higher figure. Stakeholders thought it would take around **EUR 2 800 for manufacturers to familiarise** with a new code of conduct and around **EUR 20 000 for security updates** per product (Figure 68). The pace of familiarisation and costs for manufactures are highly dependent on specific manufactures' conditions. Especially, SME will probably need more time as they are lacking the necessary IT security expertise. However, since companies are familiar with the NLF, implementing respective requirements for IT security will not pose a difficulty in itself. This can, however, be very different if another policy option was chosen.

Given the complexity of the ICT product environment, improving these guidelines (particularly security updates) could be costly. This also depends on the type of product. The cost of security updates depends on the security quality in the development. In the industrial automation area, significant testing effort may be needed before the release of a security update.

Time for preparation of security updates depends on the kind of equipment and its features. There is not one process to measure. For simple options like hidden accounts and backdoors, it should be shorter as these cases are simple. For more complex vulnerabilities, it may require more time. Another problem is how complex the offer of manufacturer is. There are players with single products and huge international companies with wide offers.

Figure 68 Code of conduct costs in comparison to UK code

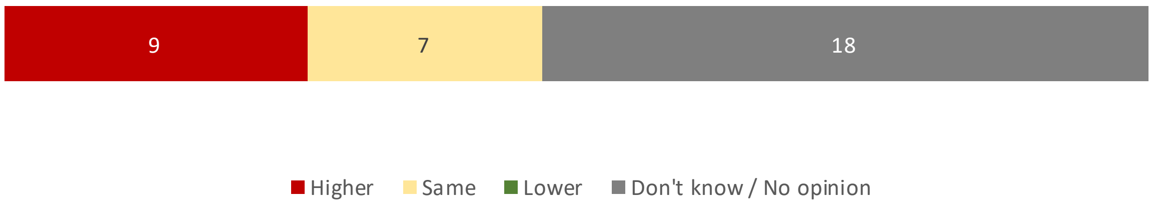


SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

Essential requirements costs

The RED IA study estimated the costs of introducing essential requirements to take two FTE, implying EUR 9 200 in staff costs. Stakeholders were asked if they foresee a lower/same/higher figure in the context of cybersecurity of ICT products. Stakeholders thought that introducing essential requirements would take **more than EUR 9 200** in staff costs per product (Figure 69). Given the high specificity of cybersecurity overall as well as difficulty of introducing of cybersecurity-related requirements, it is probable that the costs would be higher. Also, impact assessment of the essential requirements would require a lot of effort because it might require new architectures and updated security concepts. Finally, the resource pool for skilled cybersecurity personnel is much smaller than the pool for general ICT skills. The increase in demand will result in a raise in remuneration, which might push costs upwards.

Figure 69 Essential requirements costs in comparison to RED IA



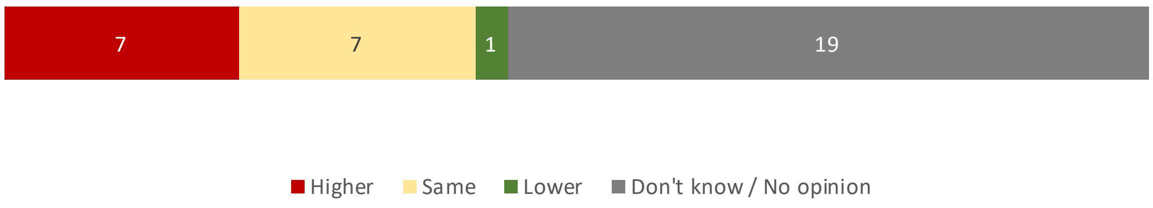
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

Market surveillance costs

The RED IA study estimated the costs of market surveillance in terms of Market Surveillance Authorities testing internet-connected devices and products amounting to EUR 5 000 - EUR 10 000 for simple equipment and up to EUR 20 000 for complex equipment. Stakeholders were asked if they foresee a lower/same/higher figure in the context of cybersecurity of ICT products. Stakeholders thought that the costs of market surveillance in terms of Market Surveillance Authorities testing internet-connected devices and products could **amount to or be higher than EUR 5 000 - EUR 10,000 for simple equipment and EUR 20 000 for complex equipment** (Figure 70). Given the high specificity of cybersecurity overall as well as difficulty of testing of cybersecurity-related requirements, it is probable that the costs would be higher. Cybersecurity equipment is complex, might need higher costs to test.

If it is about multinational market surveillance activities (as emphasised in the new Regulation (EU) 2019/1020) also the overhead for the management should be considered. Depending on the complexity of the product testing of the Market Surveillance will require at least the effort of an independent penetration testing activity.

Figure 70 Market surveillance costs in comparison to RED IA



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), DELPHI PANEL, N=34

Costs of policy options

Table 74 presents the costs of policy measures. It must be noted that the costs are mostly one-off, falling on businesses. Given the difficulty in identifying costs, they should be treated as approximations, validated by stakeholders in the Delphi panel, and are best suited for rough comparison.

Horizontal legislation could be costlier by at least 30% in comparison to Voluntary measures. Costs of sector-specific legislation would be similar as for Horizontal legislation, but concentrated on specific ICT products, risk levels or sectors selected. Costs of Mixed approach would depend on the combination of regulatory and voluntary measures but is likely to be lower than the full Horizontal legislation.

Table 74 Costs of policy options

Policy Options	Policy Measures	Policy Measure costs
Voluntary measures	Self-assessment	> EUR 18 400
	Cybersecurity label	Testing phase: EUR 10 000 - 30 000 Inspection: EUR 700
	Code of conduct	Familiarisation: EUR 2 800 Security updates: EUR 20 000
	Total upper bound	EUR 71 900
Mixed approach: *depending on the combination of regulatory and voluntary measures, but likely lower than the full Horizontal legislation.* **Sector-specific legislation:** *similar as for Horizontal legislation, but concentrated on specific ICT products, risk levels or sectors selected.*		
Horizontal legislation	Third-party assessment	EUR 15 000 – 50 000
	Testing (simple + complex)	EUR 15 000 – 30 000
	Essential requirements	> EUR 9 200
	Market surveillance	EUR 5 000 - 20 000
	Total upper bound	EUR 109 000

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

Table 75 Summary table of impacts

Impacts	Type of impact	Option 0	Option 1	Option 2	Option 3	Option 4
Effectiveness and social impacts						
Specific Objectives	Qualitative	**(-) Small negative**	**(+) Small positive**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Level of cybersecurity	Qualitative	**(-) Small negative**	**(+) Small positive**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Material and non-material safety	Qualitative	**(≈) Negligible effect**	**(≈) Negligible effect**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Choice of reliable and secure ICT products	Qualitative	**(≈) Negligible effect**	**(+) Small positive**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Trust in ICT products and the Digital Single Market	Qualitative	**(-) Small negative**	**(+) Small positive**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Efficiency and economic impacts						
Overall impact on costs	Qualitative	**(≈) Negligible effect**	**(≈) Negligible effect**	**(---) Highly negative**	**(-) Small negative**	**(-) Small negative**
Overall cost-effectiveness	Qualitative	**(≈) Negligible effect**	**(≈) Negligible effect**	**(++) Moderate positive**	**(++) Moderate positive**	**(++) Moderate positive**
Competitiveness of the ICT industry	Qualitative	**(≈) Negligible effect**	**(+) Small positive**	**(++) Moderate positive**	**(+) Small positive**	**(+) Small positive**
Innovation in the ICT industry	Qualitative	**(≈) Negligible effect**	**(+) Small positive**	**(++) Moderate positive**	**(++) Moderate positive**	**(++) Moderate positive**
Functioning and harmonisation of the Internal Market	Qualitative	**(≈) Negligible effect**	**(-) Small negative**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Level playing field	Qualitative	**(≈) Negligible effect**	**(≈) Negligible effect**	**(+++) Highly positive**	**(+++) Highly positive**	**(++) Moderate positive**
Development of the Digital Single Market	Qualitative	**(≈) Negligible effect**	**(≈) Negligible effect**	**(+++) Highly positive**	**(+) Small positive**	**(+) Small positive**
Coherence						
	Qualitative	**(-) Small negative**	**(+) Small positive**	**(+++) Highly positive**	**(+) Small positive**	**(+) Small positive**
Fundamental rights						

	Qualitative	**(-) Small negative**	**(+) Small positive**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
EU Added value						
	Qualitative	**(-) Small negative**	**(+) Small positive**	**(+++) Highly positive**	**(++) Moderate positive**	**(++) Moderate positive**
Environmental impact						
	Qualitative	**(-) Small negative**	**(+) Small positive**	**(++) Moderate positive**	**(++) Moderate positive**	**(++) Moderate positive**

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), AUTHORS' OWN ELABORATION BASED ON LITERATURE REVIEW AND DATA COLLECTION ACTIVITIES.

Table 76 below displays the final scoring given the numerical values of the qualitative assessment.

Option 2 (Horizontal legislation) would come up as the preferred option. This result was also reflected in the targeted consultation (see Annex V – Target Consultation Results for full report). Horizontal legislation was most frequently judged by the respondents to be the most cost-effective and the most likely to contribute to the consolidation of the European Digital Single Market.

Overall, respondents to the targeted consultation frequently held the view that any regulatory action should avoid any overlaps with the CSA and duplication of efforts and that horizontal legislation with mandatory requirements applying to all ICT products covered under the NLF would generate the greatest EU added value.

Table 76 Final scoring of policy options based on the qualitative assessment

Impacts	*Option 0*	*Option 1*	*Option 2*	*Option 3*	*Option 4*
	Baseline	*Voluntary*	*Horizontal*	*Sectoral*	*Mixed*
Effectiveness and social impacts					
Specific Objectives	*-1*	*1*	*3*	*2*	*2*
Level of cybersecurity	*-1*	*1*	*3*	*2*	*2*
Material and non-material safety	*0*	*0*	*3*	*2*	*2*
Choice of reliable and secure ICT products	*0*	*1*	*3*	*2*	*2*
Trust in ICT products and the Digital Single Market	*-1*	*1*	*3*	*2*	*2*
Efficiency and economic impacts					
Overall impact on costs	*0*	*0*	*-3*	*1*	*1*
Overall cost-effectiveness	*0*	*0*	*2*	*2*	*2*
Competitiveness of the ICT industry	*0*	*1*	*2*	*1*	*1*
Innovation in the ICT industry	*0*	*1*	*2*	*2*	*2*
Functioning and harmonisation of the Internal Market	*0*	*-1*	*3*	*2*	*2*
Level playing field	*0*	*0*	*3*	*3*	*2*
Development of the Digital Single Market	*0*	*0*	*3*	*1*	*1*
Coherence					
	-1	*1*	*3*	*1*	*1*
Fundamental rights					
	-1	*1*	*3*	*2*	*2*
EU Added value					
	-1	*1*	*3*	*2*	*2*
Environmental impact					
	-1	*1*	*2*	*2*	*2*
Final score based on qualitative assessment	***-7***	***9***	***38***	***29***	***28***

Source: Study on the need of Cybersecurity requirements for ICT products (2021), Authors' own elaboration based on literature review and data collection activities.

7 Conclusions and recommendations for EU Action

7.1 Conclusions

Conclusion #1 – The current EU legislation corpus in regard to cybersecurity incidents / threats (including NLF and the Cybersecurity Act) is broad and comprehensive, but does not target ICT Products

The study found that the EU legislation to tackle cybersecurity incidents and threats and to ensure the security of key areas of economic and social activity within the European Union is broad and comprehensive. However, when analysing all NLF-related legislation and other legislation closely related to cybersecurity and data protection issues and comparing the cybersecurity objectives set out in the Cybersecurity Act Art. 51 against the identified requirements of the current EU legislation, it becomes clear that the latter is not specifically targeted at ICT products. Particularly, the analysis drew the attention on the following issues: (i) the current EU legislative framework does not cover all the security objectives set out in Art. 51 of the Cybersecurity Act; (ii) the legislation related to the NLF does not address fully the cybersecurity requirements for ICT products; (iii) the granularity of some of the requirements identified in the legislation does not guarantee the fulfilment of the security objectives and; (iv) some cybersecurity requirements addressed to service operators apply indirectly to ICT products used to operate the service. At the same time, the analysis of national legislation shows – with some exceptions – that Member States are not planning to bring forward any legislative proposal that could enhance the cybersecurity of ICT products.

Conclusion #2 – The lack of secure ICT products and the insufficient understanding among users concerning the level of cybersecurity for ICT products are the two key problems to tackle

Through several workshops, the study identified two main problems, namely, the lack of secure ICT products across the EU (i.e. Problem 1) and the insufficient understanding among users concerning the level of cybersecurity for ICT products (i.e. Problem 2). The study pointed out that the security level of ICT products varies depending on the sector under consideration. In fact, while some sectors (e.g. energy, health) are characterised both by a more comprehensive sectoral legislation and higher awareness to cybersecurity risks by manufacturers, ICT products belonging to IoT Product Category appear to be relatively more vulnerable to cyber-attacks. Moreover, the analysis showed that the insufficient understanding about level of cybersecurity for ICT products does not concern all users of ICT products in the same way. Users possess very different levels of IT skills and risk awareness.

Several root causes (i.e. problem drivers) were identified with the stakeholders as underlying the lack of secure ICT products the insufficient understanding among users (i.e. Problem 1). The Targeted Consultation results pointed out main root causes being the lack of qualified security professionals (i.e. developers), no harmonised conformity assessment across the EU, no rules for post-market surveillance, no mandatory requirements (e.g. no clear obligations for the manufacturer) and no common legal basis that sets cybersecurity requirements for ICT products. On the other hand, the presence of relevant information asymmetries between consumers and producers represents one of the main drivers for the insufficient understanding of the cybersecurity of ICT products among users. In fact, cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons), particularly when the buyer is a regular user.

Conclusion #3 – The methodology developed to assess risk profiles on ICT products showed that it is not possible to aggregate risk profiles per ICT product category, or per sector due to the heterogeneity of ICT products within a category or a sector

The research results present a set of risk cases with a preliminary risk assessment for the six established product categories in each of the five selected sectors (Smart Manufacturing, Finance, Energy-Smart grid, Transport-Ports & Airports, and Smart Home) presenting the basis for future research. The adapted methodology developed by the Project Team allowed for the development of preliminary scenarios and risk-profiles at the sector level.

The results of the study showed that the methodology is adequate to identify the risk profile for a given product. On the other hand, the methodology is not adequate to create aggregated risk profiles per ICT product category, or per sector due to the heterogeneity of ICT products within a category or a sector. Therefore, the results did not allow to target specific sectors or product categories for the development of policy options. Nonetheless, the risk profiles can influence the selection of security requirements to apply for an ICT product. Those conclusions have been taken into account when building the policy options.

Conclusion #4 – A set of essential cybersecurity requirements was defined and could be applicable for all ICT products during the entire product lifecycle

The targeted online survey confirmed that cybersecurity must be addressed during the whole lifecycle of the product through various cybersecurity-related activities. Both hardware and software – which may be present within the device natively or through additional non-embedded software, as well as on backend services – should be designed, produced, configured, maintained and decommissioned with security in mind. Security evaluation should always be part of the testing phases of the product.

In order to establish a safety baseline for all products, eight essential requirements have been proposed and rated approved overall by stakeholders during the targeted online survey. The objective of these essential requirements is to set baseline cybersecurity level common to all products marketed in the EU. Exceptions would have to be evidenced by a risk assessment carried out by the manufacturer, as defined in Blue Guide of the European Union[238]. Additionally, the study has also identified a set of security requirements. The security requirements represent more granular measures (i.e. technical or organisational measures) to be met in order to fulfil each essential requirement. The security requirements are mapped against a target risk level to clarify which measures should be applied for a given risk profile. The security requirements should be fulfilled to be compliant with Essential Requirements, however it is possible for the manufacturer to go further with additional security measures.

Conclusion #5 – 5 policy options were defined taking into account the main measures of the NLF: essential requirements, conformity assessment mechanisms, reference to standards and market surveillance provisions

The Project Team designed five policy options (baseline, voluntary measures, horizontal legislation, sectorial legislation and a mixed approach between regulatory and voluntary measures). These policy options are referenced with to the NLF and the main measures of the NLF are assessed to determine how these policy options could apply to the cybersecurity of ICT products.

The NLF measures which were identified are essential requirements, conformity assessment mechanisms, reference to standards and market surveillance provisions. They offer a range of solutions which can be applied either as regulatory measures or as voluntary measures to stakeholders involved with ICT products security.

Additional details on the mechanisms and expected results of the NLF measures have been identified through several interviews. A future legislation could leverage both the NLF and the Cybersecurity Act to enhance the security of ICT Products. (as both legislations provide a set of measures applicable to ICT products).

Conclusion #6 – Horizontal legislation (Policy Option 2) is the most preferred and impactful policy option

Horizontal legislation (Policy Option 2) is the most preferred policy option. While in comparison to the other policy options considered, Policy Option 2 may result in larger overall costs, its cost-effectiveness is also potentially the highest. Concerning effectiveness, horizontal legislation is likely to have the most positive impacts on the level of cybersecurity in ICT products, material and non-material safety, choice of reliable and secure ICT products and the trust in ICT products and the Digital Single Market. Concerning efficiency, Horizontal legislation is likely to have the most positive impacts on the competitiveness of the ICT industry, innovation in the ICT industry, functioning and harmonisation of the Internal Market, level playing field and the development of the Digital Single Market. Finally, it is expected to have positive impacts on coherence with other pieces of legislation (discussed in Chapter 2), fundamental rights, EU added value and environmental impact.

Horizontal Legislation would allow to harmonize the EU regulatory landscape and avoid overlapping requirements stemming from different pieces of legislation. In addition, Horizontal legislation is seen as creating greater security in the overall market as well as a better harmonization of the European single market, creating more viable conditions for operators aiming at entering the EU market. Furthermore, Horizontal legislation would allow to better tackle the problem drivers (policy issues) compared to the other policy options. For example, Horizontal legislation allows addressing the absence of mandatory requirements (e.g., no clear obligations for the manufacturer), or the absence of rules for post-market surveillance, with regards to cybersecurity. Moreover, Problem 2 related to the current insufficient understanding of users when it comes to cybersecurity of products would be reduced. Indeed, horizontal legislation would help reduce the asymmetry between buyers and manufacturers as by default only secured products would be placed on the market. Some of the identified measures (labelling, certification) could also help users to understand the level of security of products.

The second-best options are found to be sector-specific legislation (Policy Option 3) and the Mixed approach (Policy Option 4). They scored lower on all assessment aspects than the Horizontal legislation, but nevertheless received mostly positive feedback from the respondents. The key concern in relation to these two alternatives was associated with the possibility of fragmentation in cases of product-specific legislation, and uncertainty about the outcome of a final legislative mix.

The Targeted Consultation showed very close assessment between the Horizontal legislation (Policy Option 1) and Mixed Approach (Policy Option 4), where Mixed Approach was slightly preferred as the Policy Option that would address better the need for cybersecurity requirements for ICT products. This result should be analysed bearing in mind that the type of Mixed Approach considered to be the most appropriate to address the need for cybersecurity of ICT products is the one combining regulation applicable to all categories and risk profiles of ICT products and voluntary measures. In both cases, this means that a minimum set of measures would need to be done at horizontal level (i.e. confirming Horizontal legislation Policy Option 1) possibly complemented by additional measures in the Mixed Approach (Policy Option 4).

7.2 Recommendations

Based on the research conducted throughout the study, **the Project Team recommends to the Commission:**

1. **A more comprehensive and quantitative assessment of the preferred policy options may be conducted. As indicated in the conclusions, *Policy Option 2: Horizontal Legislation*** has been identified as the solution that is more likely to have the most positive impact, with the sector-specific legislation (Policy Option 3) and the Mixed approach (Policy Option 4) identified as the second best options. Policy option 2 is expected to provide the best result when it comes to efficiency (most positive effects on the competitiveness of the ICT sector), effectiveness (most positive effects on the level of cybersecurity of ICT products) and would be consistent with the existing legislation. Policy option 3 and 4 are also expected to have mostly positive impact but scored lower than policy option 2 in all assessment aspects with uncertainty and fragmentation being the main concerns. As part of the recommended impact assessment, **precise, granular and robust impact analysis on the different measures proposed throughout the study** (labelling, certification, essential requirements, etc.) could be performed. This impact assessment could follow what was done previously in the United Kingdom[354], in regard to ICT Product cybersecurity and would allow to select the best combination of measures.

Additional investigations could be conducted to validate and precise the way forward:

2. In addition, **the implementation of Essential Requirements and security requirements, as well as conformity assessment methods (from NLF), including certification schemes resulting from the Cybersecurity Act, could be further defined**. The study has investigated one main conformity assessment activity (as defined in the NLF). However, the certification of products (as defined in the Cybersecurity Act) could also play a role in ensuring ICT products are secure. Additionally, the mandatory aspect of certification or conformity assessment activities could be further defined and refined according to additional factors if deemed necessary (sector, risk profile, etc.). Focus groups (involving manufacturers, certification bodies, consumer groups and national authorities) could help investigate the link between certification and conformity assessment to select the best measures to include in the legislation.
3. Furthermore, additional work could be provided to clarify and/or **map the roles of market surveillance bodies roles in a possible upcoming legislation.** As many different public bodies can be involved with cybersecurity of ICT Products (cybersecurity agency, safety agency, sector-specific agencies, etc.), a framework to manage the roles and responsibilities of every involved body would be welcomed. Similarly, workshops with manufacturers and national authorities could allow to define a framework for market surveillance involvement, to be applied in each sector.

Annex I – List of secondary sources

Accenture (2017). Cost of cyber crime study 2017 - insights on the security investments that make a difference. Available at: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Accenture (2020). Innovate for cyber resilience - Lessons from leaders to master cybersecurity execution. Available at: https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf

AI for Humanity. The President of the French Republic presented his vision and strategy to make France a leader in artificial intelligence (AI) at the Collège de France on 29 March 2018. Available at: https://www.aiforhumanity.fr/en/

ANEC, BEUC (2018); Cybersecurity for Connected Products – Position Papers, ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018. Available at: https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

ANEC, BEUC (2019). Keeping consumers secure, How to tackle cybersecurity threats through EU law, BEUC-X-2019-066 - 05/11/2019. Available at: https://www.anec.eu/images/documents/position-papers/2019/ANEC-DIGITAL-2019-G-096final.pdf

ANSM (2019). ANSM's Guideline – Cybersecurity of medical devices integrating software during their life cycle. https://ansm.sante.fr/var/ansm_site/storage/original/application/d774458aa87b52d2a32d736bdc9ab526.pdf

ANSSI. EBIOS Risk Manager – The method. Available at: https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

Arabo, A. (2015) Cyber Security Challenges within the Connected Home Ecosystem Futures. Complex Adaptive Systems San Jose, CA November 2-4, 2015. https://doi.org/10.1016/j.procs.2015.09.201

Baranchuk A., Alexander B., Campbell, D., Haseeb, S., Redfearn, D., Simpson, C., Glover, B. (2018). Pacemaker Cybersecurity, Vol 138, Issue 12, Circulation. Available at: https://www.ahajournals.org/doi/abs/10.1161/CIRCULATIONAHA.118.035261

Blyte, J.M. and Johnson, S.D. (2018), Rapid evidence assessment on labelling schemes implications for consumer IoT security, PETRAS IoT Hub. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf

Blythe, J.M. Johnson, S.D (2020), What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices, Crime Science volume 9, Article number: 1 (2020).

BSA – The Software Alliance (2019). BSA Policy Principles for Building a Secure and Trustworthy Internet of Things. Available at: https://www.bsa.org/files/policy-filings/07022002iotsecpolicyprinciples_0.pdf

Bundesfinanzministeriums (BMF) mit allen Informationen zu Finanzthemen. Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs und Sicherungssysteme im Geschäftsverkehr

(Kassensicherungsverordnung KassenSichV). Available at: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Verordnungen/2017-10-06-KassenSichV.html

Cambridge Dictonary (2020), Definition of “Product Life Cycle”. Available at: https://dictionary.cambridge.org/dictionary/english/product-life-cycle

CEPS (2018), Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, Report of a CEPS Task Force, p. 1, 11. Available at: https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

Check Point Reseach (2020) Cybersecurity Report. Available at: https://pages.checkpoint.com/cyber-security-report-2020.html

Council of the European Union (2017). Council Conclusions on EU External Action on Counter-terrorism, 19 June 2017, Brussels. Available at: https://www.consilium.europa.eu/media/23999/st10384en17-conclusions-on-eu-external-action-on-counter-terrorism.pdf

Council of the European Union (2018). Conclusions of 18 October 2018, Brussels. Available at: https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf

Council of the European Union (2019). Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion", 7 June 2019. Available at: https://www.consilium.europa.eu/media/39667/st10102-en19.pdf

Council of the European Union (2020) Council Conclusions on the cybersecurity of connected devices, 2 December 2020, Brussels. Available at: https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf

CSES (2020), Impact Assessment on Increased Protection of Internet Connected Radio Equipment and Wearable Radio Equipment.

Cyber Security for Europe (2020). D6.2 Education and Training Review. Available at: https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf

Cybernews, ‘Cybersecurity Made In Europe’ label goes live, 4 November 2020. Available at: https://cybernews.com/news/cybersecurity-made-in-europe-label-goes-live/

DCMS (2018). Code of Practice for Consumer IoT. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

DCMS (2020). Meeting with Peter Stephen, Head of Security by Design.

Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, 13 August 2008, Brussels.

Directive (EEC) 85/374 of the Council of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, 25 July 1985, Brussels.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance.

Directive (EC) 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety, 15 January 2002, Brussels.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’)

Directive (EU) 2006/42 of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, 9 June 2006, Brussels.

Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, 21 June 2008, Brussels.

Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC.

Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments.

Directive 2014/40/EU of The European Parliament and of The Council, of 3 April 2014, on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC.

Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast).

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, 25 May 2014, Brussels.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 19 July 2016, Brussels.

Dodson, D. Souppaya, M., Scarfone, K. (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), NIST White Paper. Available at: https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final

Dunn, K. (2004). Automatic update risks: can patching let a hacker in?, Network Security, Volume 2004, Issue 7, Pages 5-8, ISSN 1353-4858. Available at: https://www.sciencedirect.com/science/article/pii/S1353485804001023

Durumeric, Z., Bailey, M., Halderman, J.A. (2020). An Internet-Wide View of Internet-Wide Scanning. Available at: https://mdbailey.ece.illinois.edu/publications/usesec14_scanning.pdf

ECSO (2017). Position Paper – Initial position on the EU cybersecurity package. Available at: http://www.ecs-org.eu/documents/uploads/ecso-position-paper-on-cybersecurity-package.pdf

ECSO (2020). ECSO Barometer 2020: "Cybersecurity In Light Of Covid-19 - Report on the results of surveys with ECSO members and the cybersecurity community. Available at: https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf

ECSO (2020). European Cybersecurity Certification. Available at: https://ecs-org.eu/newsroom/european-cyber-security-certification

EastWest Institute (2016). Purchasing Secure ICT Products and Services: A Buyers Guide. Available at: https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf

Eileen, Y. (2021). "Singapore widens security labelling to include all consumer IoT devices, ZDNet. Available at: https://www.zdnet.com/article/singapore-widens-security-labelling-to-include-all-consumer-iot-devices/#ftag=RSSbaffb68

ENISA. Threat and Risk Management – Cramm. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

ENISA. Threat and Risk Management – Octave. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

ENISA (2012). Appropriate security measures for smart grids. Available at: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

ENISA (2013). Recommendations for a methodology of the assessment of severity of personal data breaches. Available at: https://www.enisa.europa.eu/publications/dbn-severity

ENISA (2014) Network and Information Security in the Finance Sector. Available at ; https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector

ENISA (2015). Security and Resilience of Smart Home Environments. Available at: https://www.enisa.europa.eu/publications/security-resilience-good-practices

ENISA (2015). Threat Landscape for Smart Home and Media Convergence. Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence

ENISA (2016). Architecture model of the transport sector in Smart Cities. Available at: https://www.enisa.europa.eu/publications/smart-cities-architecture-model

ENISA (2016). Communication network interdependencies in smart grids. Available at: https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids

ENISA (2016). "Mirai" malware, attacks Home Routers. Available at: https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

ENISA (2016). Security of Mobile Payments and Digital Wallets. Available at: https://www.enisa.europa.eu/publications/mobile-payments-security

ENISA (2016). Securing Smart Airports. Available at: https://www.enisa.europa.eu/publications/securing-smart-airports

ENISA (2017). Baseline Security Recommendations for IoT. Available at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ENISA (2017). WannaCry Ransomware Outburst. Available at: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

ENISA (2018). Good Practices for Security of Internet of Things in the context of Smart Manufacturing. Available at : https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

ENISA (2018). Overview of ICT certification laboratories. Available at: https://www.enisa.europa.eu/news/enisa-news/overview-of-ict-certification-laboratories-1

ENISA (2019). Cybersecurity Skills Development in the EU. Available at: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

ENISA (2019). Good practices for cybersecurity in the maritime sector. Available at: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

ENISA (2019). Good Practices for Security of IoT - Secure Software Development Lifecycle. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

ENISA (2019). How to implement security by design for IoT, Press Release. Available at: https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot

ENISA (2019). Opinion Consumers and IoT security – ENISA Advisory Group. Available at: https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

ENISA (2019). Threat Landscape Report 2018. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

ENISA (2019). Industry 4.0 Cybersecurity: Challenges & Recommendation. Available at: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

ENISA (2019) Standardisation in Support of the Cybersecurity Certification. Available at: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i

ENISA (2020). Data breach – ENISA threat landscape. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach

ENISA (2020). Main incidents in the EU and Worldwide. ENISA Threat Landscape. 20 October 2020. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

ENISA (2020). Press release: ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, 20 October 2020. Available at: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

European Commission. Digital Economy and Society Index Report 2020 - Human Capital. Available at: https://ec.europa.eu/digital-single-market/en/human-capital-and-digital-skills

European Commission. How to put cybersecurity at the centre of society: JRC report connects the dots. 20 July 2020. Available at: https://ec.europa.eu/jrc/en/news/put-cybersecurity-at-centre-of-society#:~:text=In%20a%20speech%20to%20the,sides%20of%20the%20same%20coin.&text=That's%20because%20digitalisation%20indirectly%20exposes%20everyone's%20daily%20life%20to%20cyber%20threats

European Commission. Medical devices – Sector Overview. Available at: https://ec.europa.eu/health/md_sector/overview_en

European Commission. New legislative framework. Available at: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

European Commission (2020). The EU cybersecurity certification framework. Available at: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

European Commission (2005). Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions "I2010 – A European Information Society for growth and employment", 1 June 2005, Brussels. COM (2005) 229 final. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF

European Commission (2009). Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Brussels, 30.3.2009. COM (2009) 149 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&from=EN

European Commission (2013). Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace. JOIN (2013) 1 final. 7 February 2013, Brussels. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission (2016). The 'Blue Guide' on the implementation of EU products rules. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0726(02)&from=BG

European Commission (2016). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, Brussels, 29.1.2020. COM (2016) 410 final. Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF

European Commission (2017). Commission Staff Working Document Impact Assessment Accompanying the Document Proposal For A Regulation Of The European Parliament And Of The Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"); SWD(2017) 500 final. Available at: https://ec.europa.eu/transparency/regdoc/rep/ 10102/2017/ EN/ SWD-2017-500-F1-EN-MAIN-PART-5.PDF

European Commission (2017). Joint Communication to The European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN (2017) 450 final. 13 September 2017, Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

European Commission (2018). Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027. SWD(2018) 305 final. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD%3A2018%3A305%3AFIN

European Commission (2018), Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), 7 May 2020, Brussels. COM (2018) 246 final. Avaialable at: https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-246-F1-EN-MAIN-PART-1.PDF

European Commission (2020). Communication: Shaping Europe's Digital Future, 19 February 2020. Available at: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Commission (2020). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - Identifying and addressing barriers to the Single Market. {SWD(2020) 54 final}. Available at: https://ec.europa.eu/info/sites/info/files/communication-eu-single-market-barriers-march-2020_en.pdf

European Commission (2020). Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027. Available at: https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027

European Commission (2020). EU digital ID scheme for online transactions across Europe – Inception Impact Assessment. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

European Commission (2020). General Product Safety Directive – review – Inception Impact Assessment. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-Review-of-the-general-product-safety-directive

European Commission (2020) Joint Communication To The European Parliament And The Council The EU's Cybersecurity Strategy for the Digital Decade. JOIN (2020) 18 final. 16 December 2020, Brussels. Available at https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

European Commission (2020). White Paper on Artificial Intelligence: a European approach to excellence and trust, 19 February 2020, Brussels. COM (2020) 65 final. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission (2020). Proposal for a Regulation Of The European Parliament And Of The Council On Digital Operational Resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24 September 2020, Brussels. COM (2020) 595 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1

European Commission (2020). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions – Identifying and addressing barriers to the Single Market. COM(2020) 93 final. Available at: https://ec.europa.eu/info/sites/info/files/communication-eu-single-market-barriers-march-2020_en.pdf

European Commission (2020). MDCG 2019-16 - Guidance on Cybersecurity for medical devices. Available at: https://ec.europa.eu/docsroom/documents/41863

European Commission (2021), Better Regulation Toolbox, https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en

European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM(2021) 206 final. 2021/0106(COD). Brussels, 21.4.2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

European Commission (2021). Proposal for a Regulation of The European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. COM(2021) 281 final 2021/0136 (COD). Brussels, 3.6.2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN&qid=1622704576563

European Commission (2021). Proposal for a Regulation of The European Parliament and of the Council on machinery products. COM(2021) 202 final. 2021/0105 (COD). Brussels, 21.4.2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0202

European Parliament (2021). The EU's Cybersecurity Strategy for the Digital Decade European Parliament resolution of 10 June 2021 on the EU’s Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). P9_TA(2021)0286. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html

European Court of Auditors (2019). Briefing paper: challenges to effective cybersecurity policy. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European Economic and Social Committee (2018), Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. Available at: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

European Economic and Social Committee (2020). CCMI/172 Revision of the Machinery Directive, information report Consultative Commission on Industrial Change (CCMI) on the Revision of the Machinery Directive, CCMI/172-EESC-2020. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/information-reports/revision-machinery-directive

European Parliament (2012). Resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security. 2011/2284(INI). Avaialable at: https://www.europarl.europa.eu/sides/getDoc.do?reference=P7-TA-2012-0237&type=TA&language=EN&redirect

Eurosmart (2019). A Cartography of Security Certification Schemes/Standards for IOT. Available at: https://www.eurosmart.com/wp-content/uploads/2020/02/2020-01-27-Eurosmart_IoT_Study_Report-v1.2.pdf

Eurostat. Activities via internet not done because of security concerns. (Last access in November 2020). Available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_ax/default/table?lang=en

Eurostat. Security incidents and consequences. (Last access in November 2020). Available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en

Eurostat. Trust, security and privacy - smartphones (2018). (Last access in November 2020). Available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_sp/default/table?lang=en

FFIEC (2017). Cybersecurity Assessment Tool. Available at: https://www.ffiec.gov/cyberassessmenttool.htm

German Institute for International and Security Affairs (2019). The EU's Regulatory Approach to Cybersecurity, Research Division EU / Europe | WP NR. 02, October 2019. Available at: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_2019_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf

GSMA (2020). The internet of Things 2025. Available at: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf

Han, J. and al. (2018). Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing Using Different Sensor Types, 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, pp. 836-852. Available at: https://par.nsf.gov/servlets/purl/10082721

Heitzenrater, C. D. (2017). Software Security Investment Modelling for Decision-Support. Department of Computer Science, University of Oxford. Available at: https://ora.ox.ac.uk/objects/uuid:64ddd45e-87ab-4c92-a085-df2d0d4e22e0

Hiscox (2019). Hiscox Cyber Readiness Report. Available at: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

HP (2015). Internet of Things Security Study: Smartwatches. Available at: https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf

HSE (2020). Key statistics in the Manufacturing sector in Great Britain. Available at: https://www.hse.gov.uk/Statistics/industry/manufacturing.pdf

ICTC (2012). ICT in the financial services sector: Assessing the Human Resource Needs. Available at: https://www.ictc-ctic.ca/wp-content/uploads/2012/06/ICT-in-the-Financial-Services-Sector.pdf

IDC (2019). Available at: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Ilhan, I., Karaköse, M. (2019). Cybersecurity Framework for Requirements of Repair, Update, and Renovation in Industry 4.0, 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey. Available at: https://ieeexplore.ieee.org/document/8965488

Impkamp, H. (2018), Should Prices of Consumer Goods Be Better Indicators of Product Quality?, Journal of Consumer Policy, volume 41, pages 77–81

Internet Society (2018). IoT Security for Policymakers. Available at: https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

Internet Society (2019). The economics of the security of consumer-grade IoT products and services. Available at: https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

Internet Society (2019). The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. Available at: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

IOT Industry Report (2020), Internet of Things Market Size, Growth | IoT Industry Report 2026. Available at: https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry

ISO (2012). ISO/IEC 17065. Available at: https://www.iso.org/standard/46568.html

ISO (2013). Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes. Available at: https://www.iso.org/standard/55087.html

ISO (2015). The Role of an Accreditation Body. Available at: https://isoupdate.com/resources/the-role-of-an-accreditation-body/#:~:text=Regarding%20the%20quality%20of%20products,improvement%20in%20their%20respective%20field.

ISO (2020). ISO/IEC 17000. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:en

ITU (2015). Measuring the Information Society Report, International Telecommunication Union. Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

James, M. & Szewczyk, P. (2016). Survey on remnant data research: the artefacts recovered and the implications in a cyber security conscious world. In Valli, C. (Ed.). (2016). The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia (pp.57-65). Available at: https://ro.ecu.edu.au/adf/168/

Japanese Patent Office (2017). ICT classification of the Japan Patent Office. Availablea at: https://www.researchgate.net/publication/313852860_ICT_A_new_taxonomy_based_on_the_international_patent_classification

JavaPoint. Types of Cyber Attackers. Available at: https://www.javatpoint.com/types-of-cyber-attackers

Johnson Shane D., *et. al.* (2020), The impact of IoT security labelling on consumer product choice and willingness to pay. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

Jøsang A., Ødegaard M., Oftedal E. (2015). Cybersecurity Through Secure Software Development. In: Bishop M., Miloslavskaya N., Theocharidou M. (eds) Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham. Available at: https://link.springer.com/chapter/10.1007/978-3-319-18500-2_5

JRC (2017). Smart grid projects outlook 2017. Available at: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/smart-grid-projects-outlook-2017-facts-figures-and-trends-europe

Kaspersky (2015). Black Hat USA 2015: The full story of how that Jeep was hacked. Available at: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

Kaspersky Labs (2015). Industrial control systems vulnerabilities statistics. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

Keary, E., Manico, J. (2016). Secure Development Lifecycle, OWASP. Available at: https://owasp.org/www-pdf-archive/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf

Lee, E. (2008). Cyber Physical Systems: Design Challenges. Electrical Engineering and Computer Sciences. Available at: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.pdf

Leverett E., Clayton R. and Anderson R, (2017). Standardization and Certification of the Internet of Things. Available at: https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

Li, H., Dong, K., Jiang, H., Sun, R., Guo, X., Fan, Y., (2017). Risk Assessment of China's Overseas Oil Refining Investment Using a Fuzzy-Grey Comprehensive Evaluation Method. Sustainability 2017, 9(5), 696; https://doi.org/10.3390/su9050696

McKinsey (2017). Shifting gears in cyber security for connected cars. Available at: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx

METI (2019). Cyber/Physical Security Framework (CPSF) Formulated. Available at: https://www.meti.go.jp/english/press/2019/0418_001.html

METI (2020). Meeting with Mr. OKUYA Toshikazu, Director of Cybersecurity Division.

METI (2020). Trade and Industry, IoT Security Safety Framework Securing the Trustworthiness of Mutual Connections between Cyberspace and Physical Space.

Ministero dello Sviluppo Economico (2020). Proposte per una Strategia italiana per l'intelligenza artificiale. Available at: https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf

Mitrakas A. (2020). The EU cybersecurity certification framework: performance highlights", ENISA presentation at the Cybersecurity@CEPS Summit 2020, 2 December. Available at: https://www.ceps.eu/ceps-events/cybersecurityceps-summit-2020/

Morize, A., Pointerau, R. (2020). Connected Device Life Cycle: How does it impact the viability of IoT projects?, Wavestone. Available at: https://www.wavestone.com/en/insight/connected-device-life-cycle/

Motlagh, N.H., Mohammadrezaei, M., Hunt, J., Zaker, B., (2020). Internet of Things (IoT) and the Energy Sector. Energies 2020, 13(2), 494; https://doi.org/10.3390/en13020494

National Institute of Standards and Technology (2012). Guide for Conducting Risk Assessments. Available at : https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

National Technical Authority for Information Assurance (2009). HMG IA Standard No. 1, Technical Risk Assessment. Available at : https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.177.1833&rep=rep1&type=pdf

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST (2020). NIST Cybersecurity for IoT Program. Available at: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

NTIA (2019). Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM). Available at: https://www.ntia.doc.gov/files/ntia/publications/framingsbom_20191112.pdf

OECD (1992). Guidelines for the security of Information systems. Available at: https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

OECD (2019), Summary Report of the Inaugural Event Global Forum on Digital Security for Prosperity, page 10. Available at: https://www.oecd-ilibrary.org/docserver/3206c421-en.pdf?expires=1608987015&id=id&accname=guest&checksum=B53B49F203539AE51BB6B03F541513F2

OECD (2003). Working Party on Indicators for the Information Society: A proposed classification of ICT goods, Organisation for Economic Co-operation and Development, 13 November 2003. Available at: http://www.oecd.org/digital/ieconomy/22343094.pdf

OECD (2012). ICT Applications for the Smart Grid. Available at: https://www.oecd-ilibrary.org/science-and-technology/ict-applications-for-the-smart-grid_5k9h2q8v9bln-enOECD (2015), Internet of Things: seizing the benefits and addressing the challenges, OECD Digital Economy Policy Papers

OECD (2018). Financial Markets, Insurance and Private Pensions: Digitalisation and Finance. Available at: https://www.oecd.org/competition/financial-markets-insurance-and-pensions-2018.htm

OECD (2021). Forthcoming study Understanding the digital security of products: an in-depth analysis.

Orgalim (2019), Position Paper - Building a real European Single Market for Cybersecurity: A call for a consistent approach – guiding principles. Available at: https://orgalim.eu/sites/default/files/attachment/Orgalim%20Position%20Paper%20-%20Building%20a%20real%20European%20Single%20Market%20for%20Cybersecurity%20.pdf

ORGALIM (2020). Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework, Policy Paper, 9 November. Available at: https://orgalim.eu/position-papers/digital-transformation-proposal-horizontal-legislation-cybersecurity-networkable

Palo Alto Networks (2020). The 2020 Unit 42 IoT Threat Report, Palo Alto Networks. Available at: https://start.paloaltonetworks.com/unit-42-iot-threat-report

Ping Identity (2019). Annual Survey, Consumers Hold Companies Responsible for Data Protection, Press Release. Available at: https://www.pingidentity.com/fr/company/press-releases-folder/2019/consumers-stop-engaging-brand-data-breach.html

Publication of an update to the list of national standardisation bodies pursuant to Article 27 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council on European standardisation 2020/C 104/03.

Rastogi, A., Nygard, K.E. (2017). Cybersecurity Practices from a Software Engineering Perspective, International Conference on Software Engineering Research and Practice. Available at: https://www.semanticscholar.org/paper/Cybersecurity-Practices-from-a-Software-Engineering-Rastogi-Nygard/a3b7acc1ceaae5a598f6e3322e6998cf8cf55ac1

Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC,13 August 2008, Brussels.

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, 13 August 2008, Brussels.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 4.May 2016, Brussels.

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 5 April 2017, Brussels.

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency.

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 on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, 7 June 2019, Brussels.

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, 4 July 2018, Brussels.

Riel, A., Kreiner, C., Kreiner, G., Messnarz, R. (2017). Integrated design for tackling safety and security challenges of smart products and digital manufacturing, CIRP Annals, Volume 66, Issue 1. Available at: https://hal.archives-ouvertes.fr/hal-01964583

Scott, T. (2018). Supply chain cybersecurity: A Report on the Current Risks and a Proposal for a Path Forward. Available at: https://www-file.huawei.com/-/media/corporate/pdf/trust-center/supply-chain-cybersecurity.pdf?la=en-us

Scottish Government. Public Procurement. Available at: https://blogs.gov.scot/public-procurement/2020/02/18/improving-procurement-cyber-security/

Sharbaf, M. (2020). Cybersecurity Awareness in IoT Threats. Available at: https://www.computer.org/publications/tech-news/events/cybersecurity-month-2020/awareness-iot-threats

Sherman, E., (2015). The reason companies don't fix cybersecurity. CBS News, 12 March 2015. Avaialable at: https://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

Squicciaini, M. (2017). ICT: A new taxonomy based on the international patent classification. DOI: 10.1787/ab16c396-en

Steinberg, S., (2019). Cyberattacks now cost companies $200,000 on average, putting many out of business. CNBC 13 October 2019. Available at: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Steenkamp, J.B. (1988) The relationship between price and quality in the marketplace, De Economist volume 136, pages 491–507

The Hague Security Delta (2020). European Cybersecurity Perspectives 2020. Available at: https://www.thehaguesecuritydelta.com/media/com_hsd/report/281/document/European-Cyber-Security-Perspectives-KPN-2020.pdf

Tipton, S. (2020). Cybersecurity Maturity Model Certification (CMMC) and Why You Should Care. Available at: https://www.tripwire.com/state-of-security/regulatory-compliance/cybersecurity-maturity-model-certification-cmmc/

Traficom – National Cybersecurity Centre (2020). Application Statement of compliance for the Cybersecurity Labels. Available at: https://tietoturvamerkki.fi/files/statement-of-compliance-for-the-cybersecurity-label.pdf

UNECE, Automated driving. Available at: https://unece.org/background-6

United Nations (2007). Manual for the Production of Statistics on the Information Economy. Available at: https://unctad.org/webflyer/manual-production-statistics-information-economy-2009-revised-edition

United Nations (2008). International Standard Industrial Classification of All Economic Activities: Revision 4, United Nations, New York. Available at: https://unstats.un.org/unsd/publication/seriesm/seriesm_4rev4e.pdf

United Nations (2010). International Seminar on Information and Communication Technology Statistics, 19 - 21 July 2010, Seoul, Korea. Available at: https://unstats.un.org/unsd/ict/ICT_Seminar_documents.asp

United Nations (2015). Central Product Classification (CPC): Version 2.1, New York. Available at: https://unstats.un.org/unsd/classifications/Family/Detail/1074

United Nations, Economic and Social Council (2020). Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. Item 4.12.5 of the provisional agenda. 181st session. Geneva, 23-25 June 2020. Available at: https://undocs.org/ECE/TRANS/WP.29/2020/80

Venson, E., Guo, X., Yan, Z., Boehm, B., (2019). Costing Secure Software Development - A Systematic Mapping Study. In Proceeding of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom. ACM, NewYork,NY, USA, 11 pages. https://doi.org/10.1145/3339252.3339263

Venson, E., Alfayez, R., Gomes, M., Figueiredo, R., Boehm B., (2019) The Impact of Software Security Practices on Development Effort: An Initial Survey.

Which, The smart video doorbells letting hackers into your home, 23 November 2020. Available at: https://www.which.co.uk/news/2020/11/the-smart-video-doorbells-letting-hackers-into-your-home/

White&Case (2019). Germany's Draft Bill on IT Security 2.0 – Extended BSI Authorities, Stricter Penalties and New Obligations on Providers. Available at: https://www.whitecase.com/publications/article/germanys-draft-bill-it-security-20-extended-bsi-authorities-stricter-penalties

World Intellectual Property Organisation (2008). Concept of a Technology Classification for Country Comparisons. Available at : https://www.wipo.int/export/sites/www/ipstats/en/statistics/patents/pdf/wipo_ipc_technology.pdf

World Economic Forum (2020). The Global Risks Report 2020. Available at : https://www.weforum.org/reports/the-global-risks-report-2020

World Energy Council (2018). The Role of ICT in Energy Efficiency Management. Available at: https://www.worldenergy.org/assets/downloads/20180420_TF_paper_final.pdf

WRAP (2020). Smart Devices & Secure Data Eradication: the Evidence. Available at: https://www.wrap.org.uk/sites/files/wrap/Data%20Eradication%20report%20Defra.pdf

Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., Baccelli. E. (2019). Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check. IEEE Access, IEEE, 2019, 7, pp.71907-71920. ff10.1109/ACCESS.2019.2919760ff. ffhal-02351794f? Available at: https://ieeexplore.ieee.org/document/8725488

ZVEI (2020). Horizontal Process Requirements for the Security Life-Cycle Management of IoT Products. Discussion Paper. Available at: https://www.zvei.org/en/press-media/publications/horizontal-process-requirements-for-the-security-life-cycle-management-of-iot-products

Annex II – ICT Product List

Smart Manufacturing

Table 77 List of ICT products classified by common categories – Smart manufacturing

ID	CPC ref.	ISIC ref.	ICT Category	Description
1.			**End Devices**	
1.1	45261	2620	Sensors and cameras	They detect and measure events and transmit the info
1.2	45230	2620	Safety Instrument Systems	They consist of sensors, solvers and actuators whose objective is the safety in case of violation of current conditions.
1.3	45269	2620	Actuators	They interact with the environment by moving or controlling a mechanism or systems.
1.4	45220	2620	Mobile devices	These portable devices can be operated by hand. They run mobile applications enabling operators to perform various tasks.
1.5	45230	2620	Smart robots, Automated guided vehicles	These industrial robots are designed to perform complex tasks with smart capabilities, such as the ability to learn from errors and improve their performance.
2			**Servers and Systems**	
2.1	47813	5820	Historians	These software systems gather data from industrial devices and store them in specialised databases.
2.2	45240	2620	App servers	These computers host applications
2.3	45240	2620	Database servers	These servers are used as repositories for event information provided by sensors, agents, and management servers.
2.4	47813	5820	Enterprise op. systems	These systems integrate information from various parts of an organisation.
2.5	45240	2620	Manufacturing op. systems	These systems automate production control and process automation using network computing, bridging the gap between business and plant-floor.
2.6			**ICS (Industrial Control System)**	
2.6.1	45240	2620	PLCs (Programmable Logic Controller)	These specialised industrial computers are used to automate control functions within the industrial network
2.6.2	45240	2620	RTUs (Remote Transmission Unit)	They monitor field parameters and send data to the central station.
2.6.3	45240	2620	DCS (Distributed Control System)	These control systems distribute intelligence about the controlled process instead of relying on a single central unit.
2.6.4	45240	2620	SCADA (Supervisory Control and Data Acquisition)	These systems are used to collect data from industrial assets and processes, their visualisation, supervision and control.
2.6.5	47315	2620	End user interfaces	These control panels and dashboards allow the operators to monitor and control PLCs, RTUs and other electronic devices.
3.			**Networks**	
3.1	47211	2630	Routers	These networking devices forward data packets between different networks in industrial environments.
3.2	47212	2630	IoT Gateways	These network nodes are used to interface with another network from an IoT environment using different protocols.

ID	CPC ref.	ISIC ref.	ICT Category	Description
3.3	47212	2630	Switches	These network components filter and forward packets within the local area network.
3.4	47212	2630	Wireless Access Points	These components enable wireless devices to connect to a wired network using Wi-Fi, or related standards.
3.5	84140	6120	Firewall	These network security devices or systems control network traffic between networks or between a host and a network based on predetermined rules.
3.6	84140	6120	Protocols	They define the set of rules on how two or more IoT devices communicate over a given channel.
3.7	45230	2620	Power supply	It supplies electric power to an IoT device and its internal components.
4			**Programs for decision support**	
4.1	83159	6311	AI and Machine Learning	These terms describe the ability of a machine to perform tasks typical for intelligent beings.
5			**Security**	
5.1	47813	5820	SIEM (Security Information and Event Management)	These applications are used to collect and aggregate security data from various system components and render them in the form of meaningful information via a single interface.
5.2	47829	5820	IDS/IPS (Intrusion Detection System)	These systems enable automatic monitoring of the events that occur in a computer system or network and their analysis for signs of possible incidents. In addition, IPS may execute actions in an attempt to stop detected incidents.
6			**Software**	
6.1	47821	5820	Program (code)	These programs are written for devices within an IoT ecosystem to achieve specific technological objectives, including PLC logic, SCADA applications, HMI applications, industrial robot programs, etc.
6.2	47811	5820	Operative system	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run.
6.3	47821	5820	Mobile app	These programs run on mobile devices, such as tablets and smartphones, which are used for remote supervision and control of a process
6.4	47812	5820	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.
6.5	47811	5820	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate.

Finance

Table 78 List of ICT products classified by common categories – Finance

ID	CPC ref.	ISIC ref.	ICT Category	Description
1			**End devices**	
1.1	87332	6209	Smart cards	Companies that is responsible for the integration of online payment methods in e-commerce stores. PayPal, MasterCard, Visa or American Express stand out.
1.2	45142	2620	ATMs	Machine connected by computer with bank entities that allows the customer to carry out certain banking operations by means of a magnetic card or book that is assigned a personal password.
1.3	45261	2620	Sensors and cameras	They can detect in cars the driver's behaviour on the road, and this information can be used to determine the premiums for auto insurance.
1.4	45220	2620	Mobile devices	These portable devices can be operated by hand. They run mobile applications enabling operators to perform various tasks.
2			**Software**	
2.1	84394	6312	Online banking apps and webs	It allows a user to conduct financial transactions via the Internet. (Bank apps and websites).
2.2	84394	6312	Electronic commerce apps and webs	It consists in the purchase and sale of products or services over the internet, such as social networks and other web pages. (Amazon or Aliexpress)
2.3	87332	6209	Cryptocurrency	Cryptocurrencies can be used as regular currency, and can be managed with digital wallets stored on a smartphone. All transactions are permanently recorded on the block chain.
2.4	84394	6312	Websites and online courses	They can facilitate consumer access to financial information and training.
2.5	83159	6311	Budget, retirement planning and self-commitment tools	They can help consumers to better plan their spending and savings and address their own behavioural biases.
2.6	84394	6312	Digital platforms	They can be used to help consumers to keep track of their finances and help consumers to compare financial products and decide on those products in which to invest.
2.7	84394	6312	Direct trading and investment platforms	The facilitate access to markets for both institutional investors and retail consumers. For institutional investors, these platforms are reducing reliance on market makers for trading purposes. For retail investors, trading and investing can be done at a much lower price than going through an intermediary, and some platforms even offer ready-made professionally designed portfolios.
2.8	84394	6312	Social trading platforms	They can allow investors to automatically copy the trading strategies of traders that they choose to follow.
2.9	84394	6312	Robo-advice platforms	They offer investment and portfolio management services which can automatically trade to maintain the desired risk profiles of portfolios or to realise investment losses for tax purposes. They can also use algorithms to recommend a certain investment strategy given an investor's profile or risk.
2.10	83141	6201	Risk app	Applications are also being developed to facilitate risk management functions.
2.11	47812	5820	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.

ID	CPC ref.	ISIC ref.	ICT Category	Description
2.11	47811	5820	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate.
3			**Programs for decision support**	
3.1	83141	6201	Algorithms	Their application to trading and the speed with which transactions can be executed has enabled high-frequency trading.
3.2	83159	6311	AI	It recognises patterns and predicts which investments will be high future performers.
3.3	83141	6201	Facial recognition	It can be used to estimate the health and age of an individual for the underwriting of life insurance.
3.4	83159	6311	Health AI	It can be used to analyse photos to identify certain medical conditions or the health of individuals.
4			**Security**	
4.1	83159	6311	Data encryption	To protect digitally stored data
4.2	83159	6311	Biometric technology	It can be used to improve identity verification and authentication to reduce the risk of stolen passwords or falsified transactions.
4.3	83159	6311	Data analytics	It can be used to detect irregular patterns and pinpoint if fraud has occurred
4.4	83159	6311	Distributed Ledger Technology (DLT)	It could increase the transparency of transactions, making them easier to track and control, and also reduce the risk of falsified transactions.
5			**Networks**	
5.1	47211	2630	Routers	These networking devices forward data packets between different networks in industrial environments.
5.2	47212	2630	IoT Gateways	These network nodes are used to interface with another network from an IoT environment using different protocols.
5.3	47212	2630	Switches	These network components filter and forward packets within the local area network.
5.4	47212	2630	Wireless Access Points	These components enable wireless devices to connect to a wired network using Wi-Fi, or related standards.
5.5	84140	6120	Firewall	These network security devices or systems control network traffic between networks or between a host and a network based on predetermined rules.
5.6	84140	6120	Protocols	They define the set of rules on how two or more IoT devices communicate over a given channel.
5.7	84290	6120	Online adds	They're often targeted to the profile of their viewers, which is inferred from their online behaviour and browsing habits.
5.8	84290	6120	Regular communications	Text message reminders to contribute to a savings plan or pension fund or to pay bills.
5.9	84190	6120	Customer support	Chat bots or virtual reality sessions with an advisor.

Energy (Smart grid)

Table 79 List of ICT products classified by common categories – Energy (Smart grid)

ID	CPC ref.	ISIC ref.	ICT Category	Description
1			**End devices**	
1.1	45261	2620	Sensors and sensor network	At transformers and substations or at customers' homes. They enable real time pricing, monitor the functioning and the health of grid devices. They provide outage detection and detect power quality disturbances. Control centres can thus immediately receive accurate information about the actual condition of the grid
1.2	45230	2620	Smart meters	They allow for real-time determination and information storage of energy consumption and provide 'the possibility to read consumption both locally and remotely.
1.3	45220	2620	End user interface	Customers can indicate preferences regarding vehicle charging and availability as well as for realising monetary incentives. Web portals and mobile applications can provide pricing information accurately.
1.4	45220	2620	Mobile devices	These portable devices can be operated by hand. They run mobile applications enabling operators to perform various tasks.
2			**Networks**	
2.1	47211	2630	Routers	These networking devices forward data packets between different networks in industrial environments.
2.2	47212	2630	IoT Gateways	These network nodes are used to interface with another network from an IoT environment using different protocols.
2.3	47212	2630	Switches	These network components filter and forward packets within the local area network.
2.4	47212	2630	Wireless Access Points	These components enable wireless devices to connect to a wired network using Wi-Fi, or related standards.
2.5	84140	6120	Firewall	These network security devices or systems control network traffic between networks or between a host and a network based on predetermined rules.
2.6	84140	6120	Protocols	They define the set of rules on how two or more IoT devices communicate over a given channel.
3			**Programs for decision support**	
3.1	83141	6201	Algorithms	Their application to trading and the speed with which transactions can be executed has enabled high-frequency trading.
3.2	83159	6311	AI	It recognises patterns and predicts which investments will be high future performers.
4			**Servers and systems**	
4.1	47813	5820	Historians	These software systems gather data from industrial devices and store them in specialised databases.
4.2	45240	2620	App servers	These computers host applications
4.3	45240	2620	Database servers	These servers are used as repositories for event information provided by sensors, agents, and management servers.

ID	CPC ref.	ISIC ref.	ICT Category	Description
4.4	45240	2620	PLCs (Programmable Logic Controller)	These specialised industrial computers are used to automate control functions within the industrial network
4.5	45240	2620	RTUs (Remote Transmission Unit)	They monitor field parameters and send data to the central station.
4.6	45240	2620	SCADA (Supervisory Control and Data Acquisition)	These systems are used to collect data from industrial assets and processes, their visualisation, supervision and control.
5			**Security**	
5.1	47813	5820	SIEM (Security Information and Event Management)	These applications are used to collect and aggregate security data from various system components and render them in the form of meaningful information via a single interface.
5.2	47829	5820	IDS/IPS (Intrusion Detection System)	These systems enable automatic monitoring of the events that occur in a computer system or network and their analysis for signs of possible incidents. In addition, IPS may execute actions in an attempt to stop detected incidents.
6			**Software**	
6.1	47821	5820	Program (code)	These programs are written for devices within an IoT ecosystem to achieve specific technological objectives, including PLC logic, SCADA applications, HMI applications, industrial robot programs, etc.
6.2	47811	5820	Operative system	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run.
6.3	47821	5820	Mobile app	These programs run on mobile devices, such as tablets and smartphones, which are used for remote supervision and control of a process
6.4	47812	5820	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.
6.5	47811	5820	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate.

Transport (ports & airports)

Table 80 List of ICT products classified by common categories – Transport (ports & airports)

ID	CPC ref.	ISIC ref.	ICT Category	Description
1			**Servers and systems**	
1.1			**OT systems and networks**	(Operational Technologies systems)

ID	CPC ref.	ISIC ref.	ICT Category	Description
1.1.1	45240	2620	Industrial control system (ICS)	For managing access and vehicles, infrastructure, terminal operations. It is composed of automatons and analysers (PLCs, RTUs), databases (Historian, MES, etc.), supervisory systems (DCS, SCADA), workstations (programming consoles, engineering workstation), maintenance systems and Safety Instrumented Systems (SIS).
1.1.2	47211	2630	ICS Communications networks & components	To ensure the communications between the ICS components: switches (managed and unmanaged), wireless access points, protocols, power supply systems (water, electricity, etc.)
1.2			**IT systems**	
1.2.1	45240	2620	Community system	System to share information on operations related to the vessels or airplanes between all the stakeholders (date of arrival or departure given by the airlines or shipping companies, mandatory declarations such as crew list, dangerous goods declarations, bookings of services, etc.).
1.2.2	45240	2620	Cargo system	This system is used to share information on operations related to the cargo and containers between all involved stakeholders (content of the cargo, localisation of a container, hour of its transfer, customs declarations, etc.).
1.2.3	45240	2620	Corporate systems	They are composed of different applications, systems, workstations and servers, common to every companies: financial, human resources (HR), communication and networks systems, emailing systems, sales and marketing systems (ERP), etc.
1.2.4	45240	2620	Terminal Operations Management Systems	They are mainly composed of: enterprise operations systems to plan and manage the logistics and operations (ERP, CRM, etc.), the OT systems specific to the terminal operations, terminal operating systems (TOS) used to optimise the logistics, transhipment and warehouse systems.
1.2.5	45240	2620	Traffic service	Traffic monitoring system
1.2.6	84140	6120	Servers	Web servers, application servers, proxy servers, mail servers, virtual servers, printers, etc.
2			**End devices**	
2.1	45240	2620	Related to facility specific lay-out	Specific fencing and access control, specific safety and security equipment, first response equipment, specific operational room, etc.
2.2	45240	2620	Related to vehicles moving	Boats, berth management systems, specific inspection and control equipment, etc.
2.3	45240	2620	Related to vehicles loading and unloading	Terminal-specific handling equipment and systems (cranes, ramps for passengers, pipelines, belt, conveyors, etc.), terminal-specific freight tracking systems (barcodes, liquid meters, RFID, seals, scales etc.), people badge or ticket scanners, plates reading systems, fault detectors in automated loading/unloading systems (leakages, shocks, jamming etc.)
2.4	45240	2620	Related to temporary storage	Internal transport systems (straddle carrier, yard, truck, chassis, etc.), storage equipment systems (pallet racks, tankage, etc.), cooled and uncooled stores, silos, tanks, switches (managed and unmanaged) for pipes and conveyor belts, wireless access points for « smart » seals and container self-localisation devices, etc.
2.5	45240	2620	Related to hinterland connectivity	To get in or out the cargo, container, vehicles or passengers, different end-devices are used to control and inspect them, and then transport them to other transport systems: control and inspection systems (scanners, inspection systems, Xray), railway station, marshalling yards for wagons, multimodal transport hubs for people (passengers, workers…), gate control equipment (plates reading, badges, barcodes reading, detectors)
2.6	45220	2620	Mobile devices	Smartphones, tablets, TETRA radios or specific devices used for logistics (scanning, etc.)

ID	CPC ref.	ISIC ref.	ICT Category	Description
3			**Networks**	
3.1	84150	6120	Radio	Radio systems (RFID, VHF, etc.) are used for communication with ships and planes, safety and security operations, logistics management, etc.
3.2	84140	6120	Protocols	Protocols are used to exchange information: EDI, API, authentication protocols, etc.
3.3	47212	2630	Switches, Routers, Hubs	Those components are used to forward packet in different manner between different networks
4			**Security**	
4.1	45240	2620	Detection systems	Video-surveillance, incident management systems, intrusion detection systems or abnormal behaviour systems.
4.2	45240	2620	Emergency communication systems	
4.3	45240	2620	Access control	Automatic gates, smart fencing systems, badging systems, access monitoring and counting systems
4.4	45240	2620	Traffic monitoring	Radar and electro-optic systems and train and truck traffic monitoring systems.
4.5	45240	2620	Surveillance & inspection	Detectors (fires, gas leaks, nuclear, etc.) and X-ray scanners
4.6	45240	2620	Evacuation	Exit route guidance, muster points, guidance screens and emergency doors
4.7	45240	2620	Identification & authentication	Face recognition systems, biometric systems and ID control portable terminals
4.8	45261	2620	Alerting	Sirens and loudspeakers
5			**Software**	
5.1	47821	5820	Program (code)	These programs are written for devices within an IoT ecosystem to achieve specific technological objectives, including PLC logic, SCADA applications, HMI applications, industrial robot programs, etc.
5.2	47811	5820	Operative system	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run.
5.3	47821	5820	Mobile app	These programs run on mobile devices, such as tablets and smartphones, which are used for remote supervision and control of a process
5.4	47812	5820	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.
5.5	47811	5820	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate.

Smart Home

Table 81 List of ICT products classified by common categories – Smart Home

ID	CPC ref.	ISIC ref.	ICT Category	Description
1			**End devices**	
1.1	45261	2620	Sensors and cameras (incl. Smart toys)	They include temperature and light sensors, microphones, humidity/gas/smoke detectors, motion sensors face recognition, etc.

ID	CPC ref.	ISIC ref.	ICT Category	Description
1.2	45220	2620	Mobile devices	They include specialised terminal, smart TV, smart phones, tablet computer, desktop computer, calendar/reminder devices, remote control handset, interface to home gateway and emergency button
1.3	45230	2620	Robotics	Vacuum cleaner, Lawn mower and Mobile robotics telepresence.
1.4	45230	2620	Home appliance	Refrigerator Washing machine, Dish washer, Food processor, Oven, Humidifier/Dehumidifier and Drinks makers
1.5	45269	2620	Actuators	Windows, doors and curtains/blinds actuators/motors
1.6	45269	2620	Other systems	Irrigation, pool control, smart toilet, central heating and air conditioning
1.7	45220	2620	Smart Speakers	
3			**Networks**	
3.1	47222	2630	Telephone	Mobile, fixed line, Voice Over Internet Protocol (VOIP) and Digital Enhanced Cordless Telecommunications (DECT)
3.2	84222	6120 6110	Internet connection	ADSL, Satellite, Fibre optic and 3G/4G
3.3	84140	6110	Cable connection	
3.4	47212	2630	Networking components	Switch, router, repeater, modem, gateway, firewall and WLAN access point
3.5	47212	2630	Tags and markers	RFID, NFC, Bluetooth, Wearable technology, SIM and Chip cards.
4			**Software**	
4.1	47821	5820	Program (code)	These programs are written for devices within an IoT ecosystem to achieve specific technological objectives.
4.2	47811	5820	Operative system	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run.
4.3	47821	5820	Mobile app	These programs run on mobile devices, such as tablets and smartphones.
4.4	47812	5820	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.
4.5	47811	5820	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate.
5	**45240**	**2620**	**Security**	Windows and door control, Alarm system, Access control, Video IP cameras, Security lighting and Door intercom.

Annex III – Risk profiles tables

Risk cases tables

Risk cases tables list the different attackers described above linked to the objectives that each of them wish to achieve through an attack. The attackers' targets are the feared events listed in the previous section. Given that the typical cybercriminal profile seeks financial gain, the impacts associated with it will be the direct theft of money or the theft of data for subsequent sale to interested agents or for blackmail. The group of attackers called hacktivists have ideological rather than economic objectives, so their objectives are more linked to the damage of equipment or the interruption of services in the case of activists who seek notoriety or the theft of critical information for malicious purposes or damage in people in the case of terrorists. The state sponsored ones aim to do the maximum possible damage to the sector and the nation (this does not have to include human losses). Although it is the most feared attacker profile since it is the one with the most resources, it is not so common for them to attack. Finally, the insider attack may involve an employee or customer seeking profit or revenge, or a contracted company. The tables also include the paths that the attackers will take to achieve their objectives. In other words, the sector vulnerabilities that attackers will exploit to achieve their goals. For example, for information theft, an insecure network may be the ideal way for an attacker to access information when it is being sent. Finally, the tools (attack method) that the attacker (risk origin) will use to exploit the vulnerability (paths) and thus achieve its objective are included. For example, if an attacker wanted to steal information taking advantage of an insecure network, he could use a MiTM attack. Once the scenario has been built, it is linked with the product categories listed in appendix that may be involved in the attack and the likelihood that each of these scenarios will be successful is evaluated, based on comments from expert interviews and Focus Groups.

Product categories risk cases tables

After gathering the information from the scenarios through desk research and complementing them with input from interviews with industry experts, the product categories have for each category, the attack scenarios in which it would be involved have been listed.

Regarding the impact level of each case, this value is directly linked to the severity of the objective. Different attacker, tools, or path does not change the severity of the target. For example, if we talk about human injuries or death, it will always be a case with the maximum level of impact, regardless of the other case variables. For this study, three levels of impact are being used: A low level refer to cases in which the consequences will not be serious and there is no safety risk for people or equipment; a medium level for cases with possible consequences for equipment and people; and a high level for cases in which the activity is stopped and there is a high probability of impact on the people safety.

Unlike the impact, which only takes into account the target objectives, to assess the likelihood the whole case is taken into account. Likelihood levels have been assigned based on expert opinions collected during the interviews. There are also three levels of likelihood: A low level for cases in which there is little chance that the attacker will carry out the attack successfully, a medium level for cases in which the attacker has a chance of successfully carrying out the attack and a high level for cases where the attacker is likely to be successful in the attack.

Smart Manufacturing

In this table below, the consequences that a cyberattack could have on the Smart Manufacturing sector are identified. Obviously, human loss or damage is always the most feared scenario. As the second least desired impact would be the theft of sensitive information, both personal data and classified information from the manufacturer. The theft of this information can compromise the entire business, now or in the future.

Table 82 Feared events list – Smart manufacturing

Feared events	Severity
Manipulation or loss of control, damage of the batch/product and infrastructure	2/3
Production processes affection or shutdown	2/3
Human injuries or death	3/3
Fraud and money steal	2/3
Sensitive and critical data theft	3/3
Systems damages or worst, destruction	2/3

Next table lists the different attackers described above linked to the objectives that each of them wish to achieve through an attack. The attackers' targets are the feared events listed in the previous section. Given that the typical cybercriminal profile seeks financial gain, the impacts associated with it will be the direct theft of money or the theft of data for subsequent sale to interested agents or for blackmail. The group of attackers called hacktivists have ideological rather than economic objectives, so their objectives are more linked to the damage of equipment or the interruption of services in the case of activists who seek notoriety or the theft of critical information for malicious purposes or damage in people in the case of terrorists. The state sponsored ones aim to do the maximum possible damage to the sector and the nation (this does not have to include human losses). Although it is the most feared attacker profile since it is the one with the most resources, it is not so common for them to attack. Finally, the insider attack may involve an employee or customer seeking profit or revenge, or a contracted company. The table also includes the paths that the attackers will take to achieve their objectives. In other words, the sector vulnerabilities that attackers will exploit to achieve their goals. For example, for information theft, an insecure network may be the ideal way for an attacker to access information when it is being sent. Finally, the tools (attack method) that the attacker (risk origin) will use to exploit the vulnerability (paths) and thus achieve its objective are included. For example, if an attacker wanted to steal information taking advantage of an insecure network, he could use a MiTM attack. Once the scenario has been built, it is linked with the product categories listed above that may be involved in the attack and the likelihood that each of these scenarios will be successful is evaluated, based on comments from expert interviews and Focus Groups.

Table 83 Risk cases list – Smart manufacturing

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Cyber-criminals	Fraud and money steal	Insecure Network	Malware, MiTM attack	Networks	2/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	2/3
	Sensitive and critical data theft	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
		Insecure Data storage	Manipulation of info, data abuse	End devices, Security	3/3
Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	1/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3
	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	Networks, Programs for decision support	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	2/3
		Insecure Data storage	Manipulation of info, data abuse	End devices, Security	2/3
	Systems damages or worst, destruction	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	2/3
		Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	2/3
State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	1/3
		Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	1/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3
	Production processes affection or shutdown	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	2/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	Networks, Programs for decision support	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
		Insecure Data storage	Manipulation of info, data abuse	End devices, Security	3/3
	Systems damages or worst, destruction	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	2/3
		Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3
Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	2/3
	Fraud and money steal	Weak or guessable passwords	Manipulation of info, data abuse	End devices, Security	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Software, Security, Networks	1/3

Table 84 Product categories risk cases – Smart manufacturing

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
End devices (Sensors and cameras, Safety instruments, Actuators, Mobile devices, Smart robots)	Cyber-criminals	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	3/3
	Cyber-criminals	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	3/3
	State-Sponsored attackers	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	3/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
and automated guided vehicles)	State-Sponsored attackers	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	3/3
	Hacktivists	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Hacktivists	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	2/3
	Insider attacker	Fraud and money steal	Weak or guessable passwords	Manipulation of info, data abuse	2/3	3/3
	Insider attacker	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	3/3
	Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	1/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3
	Cyber-criminals	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Production processes affection or shutdown	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Production processes affection or shutdown	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Security (SIEM, IDS/IPS)	Cyber-criminals	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	3/3
	State-Sponsored attackers	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	3/3
	Hacktivists	Sensitive and critical data theft	Insecure Data storage	Manipulation of info, data abuse	3/3	2/3
	Insider attacker	Fraud and money steal	Weak or guessable passwords	Manipulation of info, data abuse	2/3	3/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Production processes affection or shutdown	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
Servers & Systems (Historians, App servers, Database servers, Enterprise op. systems, Manufacturing op. systems)	Cyber-criminals	Sensitive and critical data theft	Lack of Secure Update Mechanism	Denial of Services attack	3/3	3/3
	Hacktivists	Systems damages or worst, destruction	Lack of Secure Update Mechanism	Denial of Services attack	2/3	2/3
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Secure Update Mechanism	Denial of Services attack	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Production processes affection or shutdown	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	1/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Secure Update Mechanism	Denial of Services attack	2/3	1/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Production processes affection or shutdown	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Software (Code, OS, Apps, Antivirus, Firmware)	Cyber-criminals	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	3/3
	State-Sponsored attackers	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	3/3
	Hacktivists	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Insider attacker	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	3/3
	Cyber-criminals	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Production processes affection or shutdown	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-Sponsored attackers	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Insider attacker	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Hacktivists	Human injuries or death	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	1/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Production processes affection or shutdown	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Networks (Routers, IoT Gateways, Switches, Wireless Access Points, Firewall, Protocols, Power supply)	State-Sponsored attackers	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	3/3	3/3
	Hacktivists	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	3/3	2/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	2/3
	Cyber-criminals	Fraud and money steal	Insecure Network	Malware, MiTM attack	2/3	2/3
	Hacktivists	Human injuries or death	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	1/3
	State-Sponsored attackers	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Production processes affection or shutdown	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	State-Sponsored attackers	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Insider attacker	Manipulation or loss of control, damage of the batch/product and infrastructure	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Insider attacker	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Programs for decision support (AI, Algorithms, Machine learning)	State-Sponsored attackers	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	3/3	3/3
	Hacktivists	Sensitive and critical data theft	Insecure Network	Malware, MiTM attack	3/3	2/3

Finance

Unlike the other sectors, the finance sector does not consider death or human damage as a direct consequence of a cyberattack (although it cannot be ruled out as an indirect consequence). On the other hand, it is clear that the theft of information is one of the most feared scenarios, since information from this sector is one of the most critical. Apart from this, the theft of money will obviously be a serious impact.

Table 85 Feared events list – Finance

Feared events	Severity
Money theft	3/3
Public image destruction	1/3
Customer frustration	2/3
Confidential information stealing	3/3

Table 86 Risk cases list – Finance

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Cyber-criminals	Money theft	Insecure network	Malware, MiTM attack	Security, Networks, Programs for decision support	3/3
		Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	Software, End devices	2/3
		Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	Software, End devices, Security, Networks	2/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
		Lack of user's diligence validating content in emails, messages…	Phishing, Social engineering	End devices, Software	3/3
	Confidential information stealing	Insecure network	Malware, MiTM attack	Security, Networks, Programs for decision support	3/3
		Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	Software, End devices	2/3
		Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	Software, End devices, Security, Networks	2/3
		Lack of user's diligence validating content in emails, messages…	Phishing, Social engineering	End devices, Software	3/3
		Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	Software, End devices	2/3
Hacktivists	Public image destruction	Weaknesses in protection of Denial of Service attacks	DoS attack	End devices, Software	2/3
	Confidential information stealing	Insecure network	Malware, MiTM attack	Security, Networks, Programs for decision support	2/3
		Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	Software, End devices	2/3
		Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	Software, End devices, Security, Networks	2/3
		Lack of user's diligence validating content in emails, messages…	Phishing, Social engineering	End devices, Software	2/3
		Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	Software, End devices, Security	2/3
State-Sponsored attackers	Confidential information stealing	Insecure network	Malware, MiTM attack	Security, Networks, Programs for decision support	1/3
		Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	Software, End devices	1/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
		Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	Software, End devices, Security, Networks	1/3
		Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	End devices, Software	1/3
		Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	Software, End devices, Security	1/3
Insider attacker	Money theft	Insecure network	Malware, MiTM attack	Security, Networks, Programs for decision support	3/3
		Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	Software, End devices	2/3
		Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	Software, End devices, Security, Networks	2/3
		Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	End devices, Software	3/3
	Customer frustration	Weaknesses in protection of Denial of Service attacks	DoS attack	End devices, Software	2/3

Table 87 Product categories risk cases – Finance

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
End devices (Smart cards, ATMs, Sensors and cameras, Mobile devices)	Cyber-criminals	Money theft	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	3/3
	Cyber-criminals	Confidential information stealing	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	3/3
	Insider attacker	Money theft	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	3/3
	Cyber-criminals	Confidential information stealing	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Cyber-criminals	Money theft	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Cyber-criminals	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Cyber-criminals	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Cyber-criminals	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	2/3
	Hacktivists	Confidential information stealing	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Hacktivists	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Lack of user's diligence validating content in emails, messages…	Phishing, Social engineering	3/3	2/3
	Hacktivists	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	2/3
	Insider attacker	Money theft	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Insider attacker	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	State-Sponsored attackers	Confidential information stealing	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Lack of user's diligence validating content in emails, messages…	Phishing, Social engineering	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Insider attacker	Customer frustration	Weaknesses in protection of Denial of Service attacks	DoS attack	2/3	2/3
	Hacktivists	Public image destruction	Weaknesses in protection of Denial of Service attacks	DoS attack	1/3	2/3
Security (Data encryption, Biometric technology, Data analytics, Distributed Ledger Technology (DLT))	Cyber-criminals	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	3/3
	Insider attacker	Money theft	Insecure network	Malware, MiTM attack	3/3	3/3
	Cyber-criminals	Money theft	Insecure network	Malware, MiTM attack	3/3	2/3
	Cyber-criminals	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Cyber-criminals	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	2/3
	Insider attacker	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	State-Sponsored attackers	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	1/3
Software (Online banking apps and webs, Electronic commerce apps and webs, Cryptocurrency, Websites and online courses,	Cyber-criminals	Money theft	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	3/3
	Cyber-criminals	Confidential information stealing	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	3/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
Budget, retirement planning and self-commitment tools, Digital platforms, Direct trading and investment platforms, Social trading platforms, Robo-advice platforms, Risk app, Antivirus, Firmware)	Insider attacker	Money theft	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	3/3
	Cyber-criminals	Money theft	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Cyber-criminals	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Cyber-criminals	Confidential information stealing	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Cyber-criminals	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Cyber-criminals	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	2/3
	Hacktivists	Confidential information stealing	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Hacktivists	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Lack of user's diligence validating content in emails, messages...	Phishing, Social engineering	3/3	2/3
	Hacktivists	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	2/3
	Insider attacker	Money theft	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	2/3
	Insider attacker	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	State-Sponsored attackers	Confidential information stealing	Insecure servers	Exploit of software vulnerabilities and design flaws, Malware	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	1/3

Product category	Risk cases					
	Risk origin	**Objective**	**Path**	**Attack method**	**Impact**	**Likelihood**
	State-Sponsored attackers	Confidential information stealing	Lack of user's diligence validating content in emails, messages…	Phishing, Social engineering	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Software weaknesses	Exploit of software vulnerabilities and design flaws, data abuse	3/3	1/3
	Insider attacker	Customer frustration	Weaknesses in protection of Denial of Service attacks	DoS attack	2/3	2/3
	Hacktivists	Public image destruction	Weaknesses in protection of Denial of Service attacks	DoS attack	1/3	2/3
Networks (Routers, IoT Gateways, Switches, Wireless Access Points, Firewall, Protocols, Online adds, Regular communications, Customer support)	Cyber-criminals	Money theft	Insecure network	Malware, MiTM attack	3/3	3/3
	Cyber-criminals	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	3/3
	Insider attacker	Money theft	Insecure network	Malware, MiTM attack	3/3	3/3
	Cyber-criminals	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Cyber-criminals	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	2/3
	Hacktivists	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	Insider attacker	Money theft	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	2/3
	State-Sponsored attackers	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	1/3
	State-Sponsored attackers	Confidential information stealing	Credit card weaknesses	Exploit of software vulnerabilities and design flaws, MiTM attack	3/3	1/3
Programs for decision support (Algorithms, AI, Facial recognition, Health AI)	Cyber-criminals	Money theft	Insecure network	Malware, MiTM attack	3/3	3/3
	Cyber-criminals	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	3/3
	Insider attacker	Money theft	Insecure network	Malware, MiTM attack	3/3	3/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Hacktivists	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	2/3
	State-Sponsored attackers	Confidential information stealing	Insecure network	Malware, MiTM attack	3/3	1/3

Energy (Smart grid)

Again, and as in most environments, human loss or damage is the worst case, followed, as is logical to think, by the energy supply disruption. The loss of control over the network, although it does not directly produce great impacts, can indirectly lead to catastrophic consequences.

Table 88 Feared events list – Energy (Smart grid)

Feared events	Severity
Communications and network control loss	3/3
Data theft	2/3
Energy supply disruption	3/3
Human injuries or death	3/3
Energy theft	1/3

Table 89 Risk cases list – Energy (Smart grid)

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Cyber-criminals	Data theft	Implicit trust M2M by default	MiTM attack, Malware	Networks, Security, Programs for decision support	3/3
		Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems	3/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	3/3
	Energy theft	Coexistence of legacy and new devices	Physical attack, Malware	Security, End devices, Servers and systems	3/3
		Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems	3/3
Hacktivists	Communications and network control loss	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems	2/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	2/3
	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems, Programs for decision support	2/3

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
		Commercial hardware and software	Malware, session hijacking	End devices, Software	2/3
	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	Security, End devices, Servers and systems	1/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	1/3
State-Sponsored attackers	Data theft	Implicit trust M2M by default	MiTM attack, Malware	Networks, Security, Programs for decision support	1/3
		Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems	1/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	1/3
	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	Security, End devices, Servers and systems	1/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	1/3
	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems, Programs for decision support	1/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	1/3
Insider attacker	Data theft	Implicit trust M2M by default	MiTM attack, Malware	Networks, Security, Programs for decision support	2/3
		Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	Security, End devices, Servers and systems	2/3
		Commercial hardware and software	Malware, session hijacking	End devices, Software	2/3

Table 90 Product categories risk cases – Energy (Smart grid)

Product category	Risk cases					
	Risk origin	**Objective**	**Path**	**Attack method**	**Impact**	**Likelihood**
End devices (Sensors and sensor network, Smart meters, End user interface)	Cybercriminals	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	3/3
	Cybercriminals	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	3/3
	Hacktivists	Communications and network control loss	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Hacktivists	Communications and network control loss	Commercial hardware and software	Malware, session hijacking	3/3	2/3
	Hacktivists	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Hacktivists	Energy supply disruption	Commercial hardware and software	Malware, session hijacking	3/3	2/3
	Insider attacker	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	2/3
	Insider attacker	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	2/3
	Cybercriminals	Energy theft	Coexistence of legacy and new devices	Physical attack, Malware	1/3	3/3
	Cybercriminals	Energy theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	1/3	3/3
	Hacktivists	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	3/3	1/3
	Hacktivists	Human injuries or death	Commercial hardware and software	Malware, session hijacking	3/3	1/3
	State-sponsored attackers	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	3/3	1/3
	State-sponsored attackers	Human injuries or death	Commercial hardware and software	Malware, session hijacking	3/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	State-sponsored attackers	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	1/3
	State-sponsored attackers	Energy supply disruption	Commercial hardware and software	Malware, session hijacking	3/3	1/3
	State-sponsored attackers	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	1/3
	State-sponsored attackers	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	1/3
Security (SIEM, IDS/IPS)	Cybercriminals	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	3/3
	Cybercriminals	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	3/3
	Hacktivists	Communications and network control loss	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Hacktivists	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Insider attacker	Data theft	Implicit trust M2M by default	MiTM attack, Malware	3/3	2/3
	Insider attacker	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Cybercriminals	Energy theft	Coexistence of legacy and new devices	Physical attack, Malware	1/3	3/3
	Cybercriminals	Energy theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	1/3	3/3
	Hacktivists	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	3/3	1/3
	State-Sponsored attackers	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	3/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	State-Sponsored attackers	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	1/3
	State-Sponsored attackers	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	1/3
	State-Sponsored attackers	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	1/3
Servers & Systems (Historians, App servers, Database servers, SCADA, RTUs, PLCs)	Cybercriminals	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	3/3
	Hacktivists	Communications and network control loss	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Hacktivists	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Insider attacker	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	2/3
	Cybercriminals	Energy theft	Coexistence of legacy and new devices	Physical attack, Malware	1/3	3/3
	Cybercriminals	Energy theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	1/3	3/3
	Hacktivists	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	3/3	1/3
	State-Sponsored attackers	Human injuries or death	Coexistence of legacy and new devices	Physical attack, Malware	3/3	1/3
	State-Sponsored attackers	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	1/3
	State-Sponsored attackers	Data theft	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	2/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
Software (Code, OS, Apps, Antivirus, Firmware)	Cybercriminals	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	3/3
	Hacktivists	Communications and network control loss	Commercial hardware and software	Malware, session hijacking	3/3	2/3
	Hacktivists	Energy supply disruption	Commercial hardware and software	Malware, session hijacking	3/3	2/3
	Insider attacker	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	2/3
	Hacktivists	Human injuries or death	Commercial hardware and software	Malware, session hijacking	3/3	1/3
	State-sponsored attackers	Human injuries or death	Commercial hardware and software	Malware, session hijacking	3/3	1/3
	State-sponsored attackers	Energy supply disruption	Commercial hardware and software	Malware, session hijacking	3/3	1/3
	State-sponsored attackers	Data theft	Commercial hardware and software	Malware, session hijacking	2/3	1/3
Networks (Routers, IoT Gateways, Switches, Wireless Access Points, Firewall, Protocols)	Cybercriminals	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	3/3
	Insider attacker	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	2/3
	State-sponsored attackers	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	2/3
Programs for decision support (AI, Algorithms)	Cyber-criminals	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	3/3
	Hacktivists	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	3/3	2/3
	Insider attacker	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	2/3
	State-Sponsored attackers	Data theft	Implicit trust M2M by default	MiTM attack, Malware	2/3	1/3
	State-sponsored attackers	Energy supply disruption	Communication protocols	Domain Name System attack, MiTM attack, Unauthorised access to systems	1/3	1/3

Transport

In the following table, the consequences that a cyberattack could have on the surroundings of a port or an airport are identified. Obviously, human loss or damage is always the most feared scenario. As the second least desired impact would appear the paralysis of the port or airport.

Table 91 Feared events list – Transport (ports & airports)

Feared events	Severity
Shutdow n of operations, port/airport paralysis	3/3
Human injuries or death, Kidnapping	3/3
Sensitive and critical data theft	2/3
Cargo and goods stealing	2/3
Illegal trafficking	2/3
Fraud and money steal	2/3
Systems damages or w orst, destruction	2/3
Tarnished reputation, loss of competitiveness	1/3

Table 92 Risk cases list – Transport (ports & airports)

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Cyber-criminals	Cargo and goods stealing	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	1/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Security, Networks	1/3
	Illegal trafficking	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	1/3
	Fraud and money steal	Insecure Network Services	Interception of emissions, MiTM attack, Session hijacking	Networks, Software	2/3
	Sensitive and critical data theft	Insecure Data Storage	Manipulation, abuse and theft of data	End devices	3/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	3/3
Hacktivists	Shutdown of operations, port/airport paralysis	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	2/3

	Human injuries or death, Kidnapping	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Security, Networks	2/3
	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	End devices, Servers and systems, Software	2/3
		Lack of Physical Hardening	Sabotage, manipulation of software/hardware	End devices, Servers and systems, Security, Networks	2/3
State-Sponsored attackers	Shutdown of operations, port/airport paralysis	Lack of Secure Update Mechanism	Denial of Services attack	Servers and systems	2/3
	Sensitive and critical data theft	Insecure Data Storage	Manipulation, abuse and theft of data	End devices	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	2/3
	Tarnished reputation, loss of competitiveness	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	1/3
Insider attacker	Fraud and money steal	Insecure Network Services	Interception of emissions, MiTM attack, Session hijacking	Networks, Software	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	End devices, Software	2/3

Table 93 Product categories risk cases – Transport (ports & airports)

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
End devices (Related to facility specific lay-out, Related to vehicles moving, Related to vehicles loading and unloading, Related to temporary storage, Related to hinterland connectivity, Mobile devices)	Hacktivists	Human injuries or death, Kidnapping	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	2/3
	Hacktivists	Human injuries or death, Kidnapping	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	2/3
	Cybercriminals	Sensitive and critical data theft	Insecure Data Storage	Manipulation, abuse and theft of data	2/3	3/3
	Cybercriminals	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	3/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	2/3
	State-sponsored attackers	Sensitive and critical data theft	Insecure Data Storage	Manipulation, abuse and theft of data	2/3	2/3
	State-sponsored attackers	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Insider attacker	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Cybercriminals	Cargo and goods stealing	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	Cybercriminals	Cargo and goods stealing	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
	Cybercriminals	Illegal trafficking	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	State-sponsored attackers	Tarnished reputation, loss of competitiveness	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	1/3	1/3
Servers & Systems (ICS, ICS Communications networks & components, IT systems, Community, system, Cargo system,, Corporate systems Terminal Operations Management, Systems, Traffic service)	Hacktivists	Shutdown of operations, port/airport paralysis	Lack of Secure Update Mechanism	Denial of Services attack	3/3	2/3
	Hacktivists	Human injuries or death, Kidnapping	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	2/3
	State-sponsored attackers	Shutdown of operations, port/airport paralysis	Lack of Secure Update Mechanism	Denial of Services attack	3/3	2/3
	Hacktivists	Human injuries or death, Kidnapping	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	2/3
	Cybercriminals	Cargo and goods stealing	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	Cybercriminals	Cargo and goods stealing	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
	Cybercriminals	Illegal trafficking	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
Software (Code, OS, Apps, Antivirus, Firmware)	Hacktivists	Human injuries or death, Kidnapping	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	3/3	2/3
	Cybercriminals	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	3/3
	Cybercriminals	Fraud and money steal	Insecure Network Services	Interception of emissions, MiTM attack, Session hijacking	2/3	2/3
	Hacktivists	Systems damages or worst, destruction	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	2/3
	State-sponsored attackers	Sensitive and critical data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Insider attacker	Fraud and money steal	Insecure Network Services	Interception of emissions, MiTM attack, Session hijacking	2/3	2/3
	Insider attacker	Fraud and money steal	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	2/3	2/3
	Cybercriminals	Cargo and goods stealing	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	Cybercriminals	Illegal trafficking	Use of insecure or outdated components	Malware, Software vulnerabilities exploitation	2/3	1/3
	State-sponsored attackers	Tarnished reputation, loss of competitiveness	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	1/3	1/3
Networks (Radio, Protocols, Switches, Routers, Hubs)	Hacktivists	Human injuries or death, Kidnapping	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	2/3
	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	2/3
	Cybercriminals	Fraud and money steal	Insecure Network Services	Interception of emissions, MiTM attack, Session hijacking	2/3	2/3
	Insider attacker	Fraud and money steal	Insecure Network Services	Interception of emissions, MiTM attack, Session hijacking	2/3	2/3
	Cybercriminals	Cargo and goods stealing	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3
Security	Hacktivists	Human injuries or death, Kidnapping	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	3/3	2/3

Product category	Risk cases					
	Risk origin	**Objective**	**Path**	**Attack method**	**Impact**	**Likelihood**
(Detection systems, Emergency communication systems, Access control, Traffic monitoring, Surveillance & inspection, Evacuation Identification & authentication, Alerting)	Hacktivists	Systems damages or worst, destruction	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	2/3
	Cybercriminals	Cargo and goods stealing	Lack of Physical Hardening	Sabotage, manipulation of software/hardware	2/3	1/3

Smart Home

The home environment, as in finance, does not pose the possibility of death or human harm due to a cyberattack. Any household device that has the slightest chance of causing serious harm to people is not even intended to be manufactured. However, it is the scenario with the most serious impacts. It must be understood that the domestic environment is the least susceptible to major attacks but also the least prepared. In this sense, theft of money or personal information, espionage or physical theft appear as feared impacts.

Table 94 Feared events list – Smart home

Feared events	Severity
Money theft	3/3
Customer frustration	1/3
Personal data theft	3/3
Cyberespionage	3/3
Damage or destruction of devices	2/3
Physical theft	3/3
Service disruption	2/3

Table 95 Risk cases list – Smart home

Risk origins	Target objectives	Paths	Attack method	Related products	Likelihood
Cyber-criminals	Money theft	Insecure Data storage	Manipulation, abuse and theft of data	Software	2/3
	Personal data theft	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	Network	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	Software	2/3
		Insecure Data storage	Manipulation, abuse and theft of data	Software	2/3
	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation,	Software, End devices	3/3
	Physical theft	Physical access	Physical attack	End devices, Networks, Security	2/3
Hacktivists	Service disruption	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	Network	2/3
		Insecure update	Software vulnerabilities exploitation	Software, End devices	2/3

	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	Software	2/3
State-Sponsored attackers	Service disruption	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	Network	1/3
		Insecure update	Software vulnerabilities exploitation	Software, End devices	1/3
	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	Software	1/3
Insider attacker	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	Software	3/3
	Personal data theft	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	Network	2/3
		Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	Software	2/3
		Insecure Data storage	Manipulation, abuse and theft of data	Software	2/3

Table 96 Product categories risk cases – Smart home

Product category	Risk cases					
	Risk origin	Objective	Path	Attack method	Impact	Likelihood
Software (Code, OS, Apps, Antivirus, Firmware)	Cybercriminals	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation,	3/3	3/3
	Insider attacker	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	3/3	3/3
	Cybercriminals	Money theft	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
	Cybercriminals	Personal data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Cybercriminals	Personal data theft	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3
	Hacktivists	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	3/3	2/3
	Insider attacker	Personal data theft	Insufficient Privacy Protection	Software vulnerabilities exploitation, data abuse	3/3	2/3
	Insider attacker	Personal data theft	Insecure Data storage	Manipulation, abuse and theft of data	3/3	2/3

Product category	**Risk cases**					
	Risk origin	**Objective**	**Path**	**Attack method**	**Impact**	**Likelihood**
	Hacktivists	Service disruption	Insecure update	Software vulnerabilities exploitation	2/3	2/3
	State-sponsored attackers	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	3/3	1/3
	State-sponsored attackers	Service disruption	Insecure update	Software vulnerabilities exploitation	2/3	1/3
End devices (Sensors and cameras, Mobile, devices, Robotics. Home appliance, Actuators)	Cybercriminals	Cyberespionage	Insufficient Privacy Protection	Software vulnerabilities exploitation	3/3	3/3
	Cybercriminals	Physical theft	Physical access	Physical attack	3/3	2/3
	Hacktivists	Service disruption	Insecure update	Software vulnerabilities exploitation	2/3	2/3
	State-sponsored attackers	Service disruption	Insecure update	Software vulnerabilities exploitation	2/3	1/3
Networks (Telephone, Internet connection, Cable connection, Networking components, Tags and markers)	Cybercriminals	Personal data theft	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	3/3	2/3
	Cybercriminals	Physical theft	Physical access	Physical attack	3/3	2/3
	Insider attacker	Personal data theft	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	3/3	2/3
	Hacktivists	Service disruption	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	2/3	2/3
	State-sponsored attackers	Service disruption	Insecure network	Eavesdropping/Interception/Hijacking & Nefarious Activity/Abuse	2/3	1/3
Security (Windows and door control, Alarm system, Access control)	Cybercriminals	Physical theft	Physical access	Physical attack	3/3	2/3

Annex IV – Labelling

Labelling in Finland

The National Cyber Security Centre Finland (NCSC-FI), established in 2005, develops and monitors the operational reliability and security of communications networks and services. NCSC-FI is part of Traficom, the Finnish National Transport and Communications Agency. Concerning ICT security, in particular, the Finnish Transport and Communications Agency Traficom has implemented a **program of Labels for IoT products.** The team working on the Finnish labelling system is composed of 5 members. The idea of establishing a program for cybersecurity labels for IoT systems stemmed from a long evaluation of the consistent increase of malware in connected devices over time. From 2010, when technologies such as IoT and Cloud Service developed to an adequate extent, Finland started inquiring on IoT security and in 2015 started working towards a labelling system. Finally, in 2018, Finland launched its "Future Work Program" focusing on current challenges arising from the adoption of new technologies, IoT being one of them, and created the Cybersecurity Label Program for IoT devices.

This program aims at helping consumers to make more secure choices when purchasing IoT devices or services. Indeed, the label informs purchasers that the device or service has passed an audit phase, based on the security requirements set by the NCSC-FI. Also, the Cybersecurity Label helps producers in showing their commitment to IoT security. Notably, the Cybersecurity Label applies only to consumers' applications and not to business solutions.

Using Cybersecurity Labels is voluntary. Indeed, according to the NCSC-FI, the rapid development in the field of IoT technologies and the current lack of knowledge related to the faults these systems carry on has made it challenging to adopt binding regulation. Regulations are more hardly amendable than voluntary mechanisms, and thus should be implemented once a more thorough understanding of these systems is acquired.

In this context, another aim of the Cybersecurity Label is to gather experiences on the most relevant requirements that would need to be implemented (e.g., how effective these are in mitigating threats). The Finnish government would have favoured a harmonized approach at the EU level, however, at the time of the implementation of the Cybersecurity Labels no common mechanism was available. However, in conjunction with the launch of the piloting project for cybersecurity labels, the ETSI standard was also published. Therefore, ETSI's most relevant requirements have been taken into account for drafting the Finnish cybersecurity label program.

Main Steps of the Finnish Labelling Application Process

To receive the label, a vendor must contact the NCSC-FI and fill in a statement of compliance form. Then, a threat model and a testing plan are crafted by the NCSC-FI. If the product passes the testing phase the certificate will be granted to the vendors.

More specifically, the main steps vendors should follow to receive the label are:

1. Begin the discussion with Traficom or the inspection body:
    a. To receive the right to use the Label, the device or service must be protected from the most common IoT threats.
    b. The NSCS has se**t security requirements** that must be met (see BOX 1). These requirements will be checked by a third party, which may be a security company chosen by the company and approved by Traficom.
2. Third-party inspection phase[355]
    a. The product or device must pass the inspection.
    b. The inspection will verify that the product meets the requirements and provides thorough documentation.
3. Traficom inspection review phase
    a. Traficom validates the outcome of the inspection and whether the product meets the requirements.
    b. Traficom comments on possible amendments that need to be done
4. Decision on required amendments
    a. If the received information is deemed sufficient and in conformity with the requirements, the label can be granted. If any issue remains open or the product fails to meet the requirements, the process of labelling needs to be amended.
    b. The list of required amendments is sent to the applicant and the inspection body.
5. Amendments made by the applicants
    a. To receive the label, the applicant needs to correct the shortcomings, and send the necessary proofs and documents to the inspection body and Traficom.
    b. Traficom grants label and annually monitors product compliance.
    c. After the Cybersecurity Label is granted, the company can attach it to the audited products and market the labelled product. The label cannot be used for other purposes.
    d. The product information will also be added to the Cybersecurity Label web pages.[356]

For the label to be maintained, the product is also subject to an annual review. In particular:

1. Traficom is in charge of informing the holders that the label is expiring and needs to be reviewed.
2. The holder submits information on the changes made to the product or service after the inspection.
3. If the changes are significant and affect the security of the product/service, the inspection process needs to be undertaken again. If no major changes have been made since the inspection, the process proceeds directly for approval and the continuation of the right to use the label.

If a new inspection is required, products/services go through the inspection process. Whenever approval from Traficom has been received, the right to use the label continues.

Notably, the cybersecurity label does not address devices' security only. The NCSC-FI granted a label to a mobile application also. The requirements, in this case, were borrowed from the OWASP Application Security Verification Standard (ASVS) Project, which provides a basis for testing web application technical security controls and provides developers with a list of requirements for secure development.

Established Requirements[357]

The Finnish government has envisaged several security requirements that the vendors should fulfil to acquire the Cybersecurity Label. These requirements are mapped against the ETSI Standards:

6. Where passwords are used and, in any state, other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user (ETSI 5.1-1).
7. When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates (ETSI 5.3-2). An update shall be simple for the user to apply (ETSI 5.3-3). Updates shall be timely (ETSI 5.3-8). The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update (ETSI 5.3-11). The manufacturer shall make a vulnerability disclosure policy publicly available (ETSI 5.2-1). Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period (ETSI 5.2-3).
8. The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers (ETSI 6.1).
9. Sensitive security parameters in persistent storage shall be stored securely by the device (ETSI 5.4-1). The consumer IoT device shall use best practice cryptography to communicate securely (ETSI 5.5- 1). The manufacturer shall follow secure management processes for critical security parameters that relate to the device (ETSI 5.5-8).
10. Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practices on usability (ETSI 5.12-1).

The list of requirements is relatively compact. Indeed, it is in the opinion of the Finnish government that asking vendors to fulfil too many requirements would cause most vendors to fail, and thus the Cybersecurity Label mechanism to be ineffective.

[355] The inspection can be made by Cybersecurity companies specializing in security inspections and approved by Traficom. The government actively discussed with commercial security companies available to take care of the testing phase when handling their task so that a shared understanding of what is relevant in terms of threats is developed.

[356] See: www.cy bersecuritylabel.fi

[357] Traf icom, Application Statement of compliance for the Cybersecurity Labels

Cost of the Security Labelling in Finland

Since most Finnish companies are SMEs, the government first considered establishing self-assessment procedures. However, vendors participating in the pilot of the Cybersecurity Label advocated for having the evaluation performed by a third-party. The cost of the inspection depends on the amount of work and the pricing of the inspection body, which have the right to price their work independently. Besides, the testing costs also depends on the product in question. In general terms, the testing phase's costs range between 10.000 and 30,000 euros.

The duration of the inspection varies between approximately 5 and 20 working days. The ability of the applicant to supply the required information during the inspection process significantly affects the swiftness of the process. The cost per product of the inspection includes the:

- Right to use the Label: 350 euros
- Annual review: 350 euros.

Labelling in Germany

While the German Ministry of the Interior issues several certifications for IT products and systems regarding their security functions, it also believes that, for some consumer products, it would be too expensive and partially ineffective to run a certification process. Therefore, Germany developed the IT Security Label. This lighter approach allows, on the one hand, to let customers decide whether they would like to pay in exchange for stronger security and trust in the products they buy rather than mandating to the manufacturer to acquire the certification. On the other hand, unlike the certification, which assesses the security of the product at the time when it is placed on the market, the IT Security Label allows to dynamically monitor the security of the product over time.

The IT Security Label aims to enhance consumer products' security. The IT Security Label was launched in 2020 in response to an order issued by the Bundestag in March 2017 (BT-Drucksache 18/11808). The challenge faced by Germany was that the access to the EU market could only be regulated based on European harmonized rules. As such, there was no possibility of issuing national mandatory minimum requirements for consumer products. Because of this, the Ministry of the Interior, Building and Community developed a voluntary system, where the manufacturer would be the main responsible for the security of the product, while the BSI would be responsible for the consumers' protection.

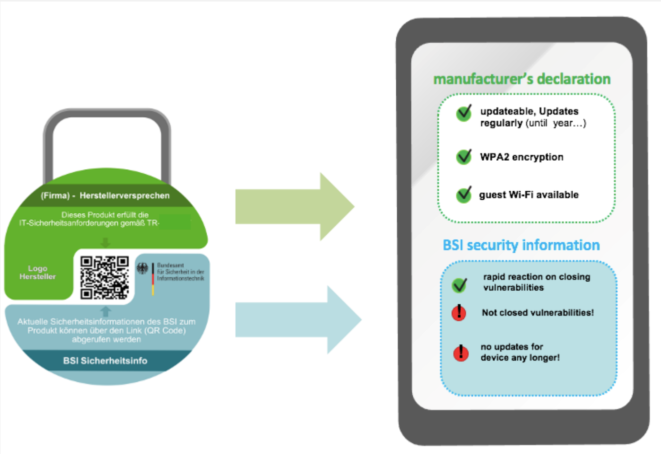
Notably, if Germany would have had the possibility to directly issue mandatory security requirements, it would have preferred this option. Whenever a manufacturer wishes to get a label, he submits his product to the BSI, the main security agency in Germany, self-attesting the product compliance with the security requirements. For its part, the BSI issues updates for the products when new vulnerabilities are discovered. Every product is marked with a QR code that allows consumers to download patches directly from the producers' website. Hence, the Label creates a direct connection between the consumer, the producer, and the BSI.

Acknowledging the lack of a standardized, understandable and up-to-date system for informing consumers about IT security that would help them decide which product to buy, Germany developed the IT Security Label. The Label is not a certification. It adds to the current certification schemes information to be provided to consumers at the level of the manufacturer declaration. The label can be released faster than the certification. Indeed, to get the label, it is sufficient only to have a manufacturer's self-declaration based on a checklist provided by the BSI. The BSI will then check whether the declaration is plausible. However, subsequent controls by the BSI will be performed to check the security of the product over time. No ex-ante control is performed by the BSI. Germany included the IT Security Label under the latest IT security law, as such, the human capital of the BSI to check for compliance would be increased. The IT Security Label consist of two components: on one hand, the manufacturer declaration of conformity with the security requirements, based on the Technical Guidelines of the BSI, on EU technical standards, or the company's standards; on the other hand, the information provided by the BSI for dynamically monitoring what are the needed updates, based on the newly discovered vulnerabilities.

To put in practice such a dynamic monitoring a QR code is placed on the product informing the purchaser of the product's security level. This information can be seen by both the customers and the vendors.

Figure below provides a draft example of how the IT Security Label looks like.

Electronic information for customer/user


(Firma) - Herstellerversprechen
Dieses Produkt erfüllt die IT-Sicherheitsanforderungen gemäß TR-
Logo Hersteller
Bundesamt für Sicherheit in der Informationstechnik
Aktuelle Sicherheitsinformationen des BSI zum Produkt können über den Link (QR Code) abgerufen werden
BSI Sicherheitsinfo
manufacturer's declaration
✓ updateable, Updates regularly (until year…)
✓ WPA2 encryption
✓ guest Wi-Fi available
BSI security information
✓ rapid reaction on closing vulnerabilities
! Not closed vulnerabilities!
! no updates for device any longer!

Source: Meeting with the German Federal Ministry of the Interior, Building and Community

The security requirements are established by the BSI through the Technical Guidelines but companies have also the freedom to come up with their standards that might be then be proposed to the BSI and eventually included in the Technical Guidelines. Notably, when drafting the Technical Guidelines, the BSI takes also into account international standards, as well as, for example, lessons learned from critical infrastructures' protections. However, it should be noted that consumer products' security should not be overloaded with unnecessary requirements. A critical factor that needs to be taken into account is the *usability* of the products. Having a highly secure product might also require having an equally sophisticated consumer to use the product. As such, security requirements need to be level up with consumers' skills.

The advantages foreseen for the IT Security Label are that the manufacturers are responsible for compliance with their declaration, which is flexible and dynamic. For their part, consumers are able to assess the security of a product before buying it. The IT security label is designed in a way to make clear that users should access the electronic leaflet on an ongoing basis. The label would otherwise be ineffective in case a product remains in a shop for several years, such as that the information provided would not be up to date anymore. *Technical requirements for Secure Broadband Router as a pilot for developing the IT security label*[358]

An example of a BSI Technical Guideline is the one for Secure Broadband Routers. Routers are considered one of the main pillars in IT products and systems' security, being the main gate between the Internet and the home network. The Technical Guideline for Secure Broadband Router served also as a pilot for developing the IT security Label.

[358] For more on this see, BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf;jsessionid=93DD61E70B4B263045615D77313C0383.1_cid503?__blob=publicationFile&v=3

The Technical Guideline defines mandatory and optional security requirements on routing devices designed for end-users. The primary addressees of the Technical Guideline are the manufacturers, but it may be of interest to retailers and end-users as well. The Technical Guideline guides manufacturers on designing and implementing a product with adequate state-of-the-art security features. Consistently, the Guideline focuses mainly on factory setting and initialized state which are the state of the router life cycle under the control of the manufacturer.

After having presented the threat model for routers, the Technical Guideline sets out several specific requirements that manufacturers should fulfil to guarantee routers' security. Among the enlisted requirements there are, for example:

- To prevent attacks on secured connections and on the router itself, all (private) cryptographic keys and secrets MUST NOT be shared by multiple devices in the factory setting and initialized state.
- In factory settings, the router SHOULD restrict access to a defined list of services provided to devices connected on the LAN and WLAN interface by the router.
- Only a minimal selection of services SHOULD be available on the LAN and WLAN interface of the router.
- In factory settings, the Extended Service Set Identifier (ESSID) SHOULD NOT contain information that consists of or is derived from data or parts of data that depend on the router model itself (e.g., model name).

The whole list of security requirements entails both provisions for the network and interfaces of the routers as well as for the functionalities that may be offered (e.g., Network Attached Storage (NAS), e-mail, Dynamic Host Configuration Protocol (DHCP), Virtual Private Network (VPN), etc.).

Cost of Labelling in Germany

The costs for companies to get the label is minimal. Companies are only charged for BSI administration costs, and they will possibly have to bear some internal costs for assessing their declaration. These costs will nonetheless be much cheaper than those related to getting a certification.

Annex V – Target Consultation Results

Introduction

This report presents the analysis of the results of the online targeted consultation, one of the multiple consultation activities feeding into the Study on cybersecurity requirements for ICT products.

Objectives

An online targeted consultation was conducted as part of this study to allow a wider audience of experts, professionals and other relevant interested parties to express their views on current EU legislation and options for future EU legislation around cybersecurity requirements for ICT products. More specifically, the targeted consultation sought views on:

1. Current issues around cybersecurity of ICT products and the appropriateness of legislation to address it (Problem definition)
2. Cybersecurity issues as per categories of ICT products and risk profiles
3. Proposed policy options for ICT Cybersecurity going forward
4. The likely impacts of the proposed policy options
5. The online targeted consultation was launched in April 2021 and ran for a period of 12 weeks, in accordance with the Better Regulation Guidelines. It closed on 21 May 2021.

Methods used

As this was a targeted consultation, potential respondents were identified from relevant institutions and organisations in the fields of ICT and cybersecurity policy based on the contacts database of DG CONNECT and our partners Wavestone, CEPS and CARSA.

A ‘snowball sampling’ method was also used whereby the invited stakeholders were encouraged to share the link to the targeted consultation within their professional networks.

The stakeholder categories targeted were as follows:

1. European Institutions
2. National Competent Authorities (NCAs)
3. ICT industry (product developers, device manufacturers, maintenance services)
4. Academic experts
5. Professional users (representing sectors that critically rely on ICT)
6. Consumer associations

The results presented in this report have been disaggregated by the above stakeholder categories where relevant (when significant disparities were observed).

Representativeness of the surveyed sample

Online surveys cannot be fully representative of European or national populations or population sub-groups or stakeholder types as they employ non-probability sampling. Therefore, from a statistical perspective, responses cannot be extrapolated to a given population, but are only representative of those who responded to the survey.

Number of responses received, broken down by stakeholder type and Member State

A total of 88 responses were received to the targeted consultation.

More than two-thirds (71%) of the respondents either represented National competent authorities (NCAs) or the ICT industry. Responses from academic experts and representatives of professional users represent 17% of the total response. A few consumer associations, the key EU-level ones, also contributed their response to this survey. Two responses were received from representatives of EU Institutions.

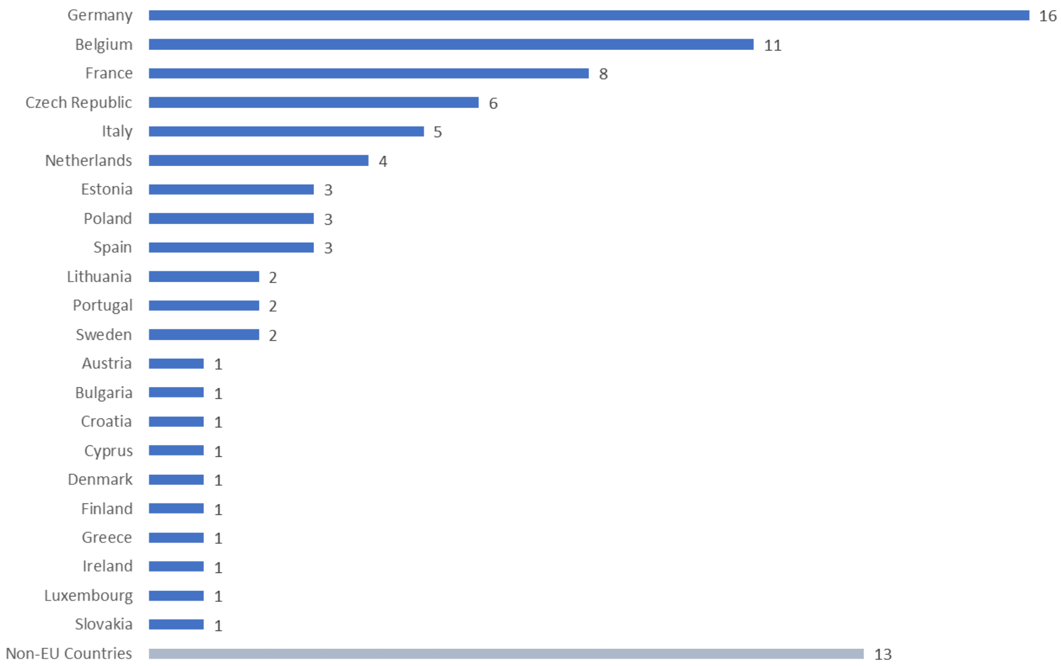
Table 97 Stakeholder types in the sample

Stakeholder type	No. of responses	% response
European Institutions	2	2%
National competent authorities	36	41%
ICT industry players	26	30%
Academic experts	8	9%
Professional users	7	8%
Consumer associations	5	6%
Other	4	4%
Total	**88**	**100%**

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

There was a total of 16 responses received from Germany, followed by 11 from Belgium, and 8 from France while 13 came from respondents in non-EU countries. There was on average very few responses from the remaining Member States and none from the following Member States: Hungary, Latvia, Malta, Romania, Slovenia. It is for these reasons that the survey responses have not been analysed by country.

Table 98 Overview of responses by country



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

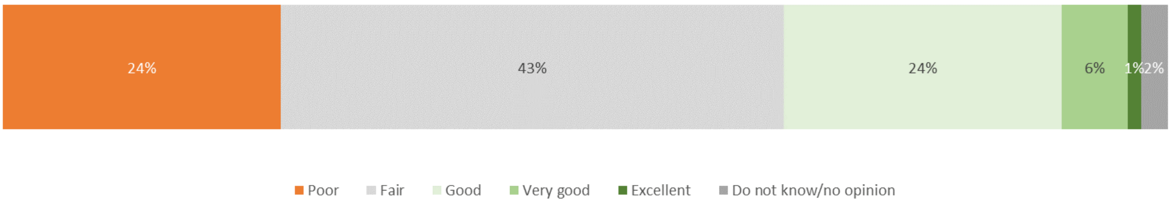
Problem definition – current cybersecurity issues

This section covers the results from the questions seeking respondents' views and experiences of cybersecurity issues and the appropriateness of current cybersecurity arrangements for ICT products.

Overall level of cybersecurity of ICT products

After being given some context on the importance of cybersecurity in ensuring the smooth functioning of the European Single Market in the digital era, the respondents were asked to rate the level of security of ICT products across the EU.

Figure 71 Q1: In your opinion, what is the level of security of ICT products available across the EU?

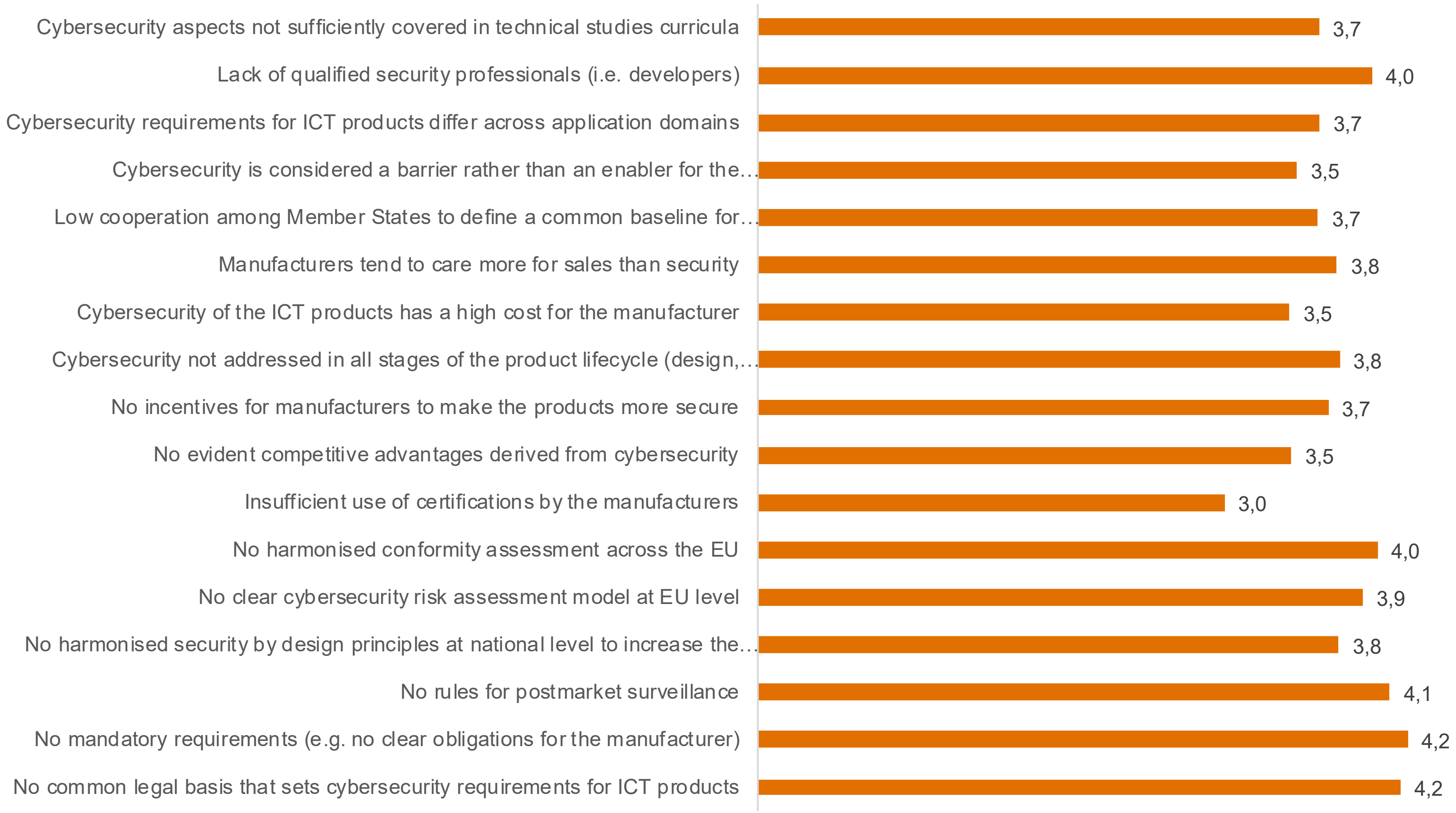


Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

A significant proportion of the respondents (43%) thought the level of security of ICT products available in the EU was fair. There was an equal proportion of respondents who thought that the level of security of ICT products is either poor or good (24%). Only 7% of the respondents thought this level to be very high or excellent.

Respondents were asked about **the reasons for inadequate security of ICT products across the EU** (Figure 72). They agreed that the reasons are the lack of qualified security professionals (i.e. developers), no harmonised conformity assessment across the EU, no rules for post-market surveillance, no mandatory requirements (e.g. no clear obligations for the manufacturer) and no common legal basis that sets cybersecurity requirements for ICT products. There were no significant differences between respondent types.

Figure 72 Q2: To what extent are the following statements a reason for inadequate security of ICT products across the EU? (1-Strongly disagree; 2-Somewhat disagree; 3-Neither agree nor disagree; 4-Somewhat agree; 5-Strongly Agree)

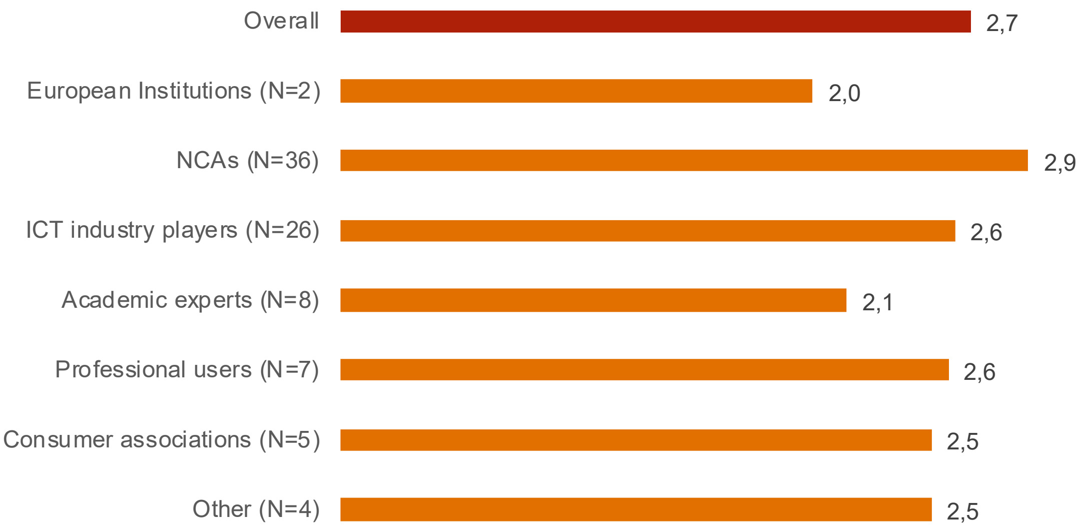


SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Awareness of ICT product security

Respondents were asked about **the level of understanding (awareness) among the professional users concerning the level of security of ICT** (Figure 73). Overall, respondents thought that the understanding is fair to good (rating 2.7 out of 5). There were no significant differences between respondent types.

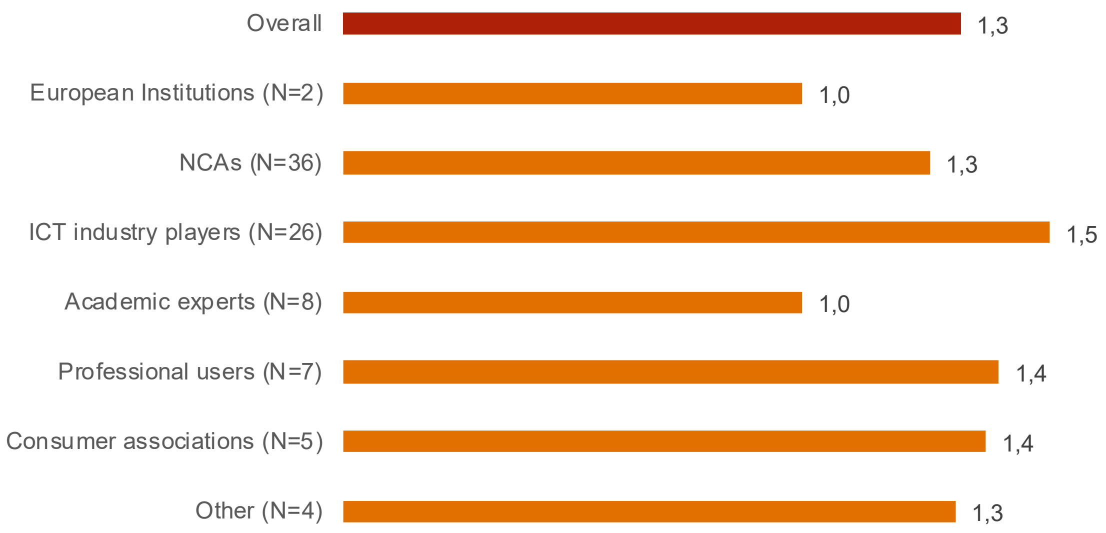
Figure 73 Q3: In your opinion, what is the level of understanding (awareness) among the professional users concerning the level of security of ICT products? (1-Poor; 2-Fair; 3-Good; 4-Very good; 5-Excellent)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021). TARGETED CONSULTATION ONLINE SURVEY, N=88.

Respondents were asked what is **the level of understanding (awareness) among regular users (citizens) concerning the level of security of ICT products** (Figure 74). Overall, respondents thought that the understanding is poor (rating 1.3 out of 5). There were no significant differences between respondent types.

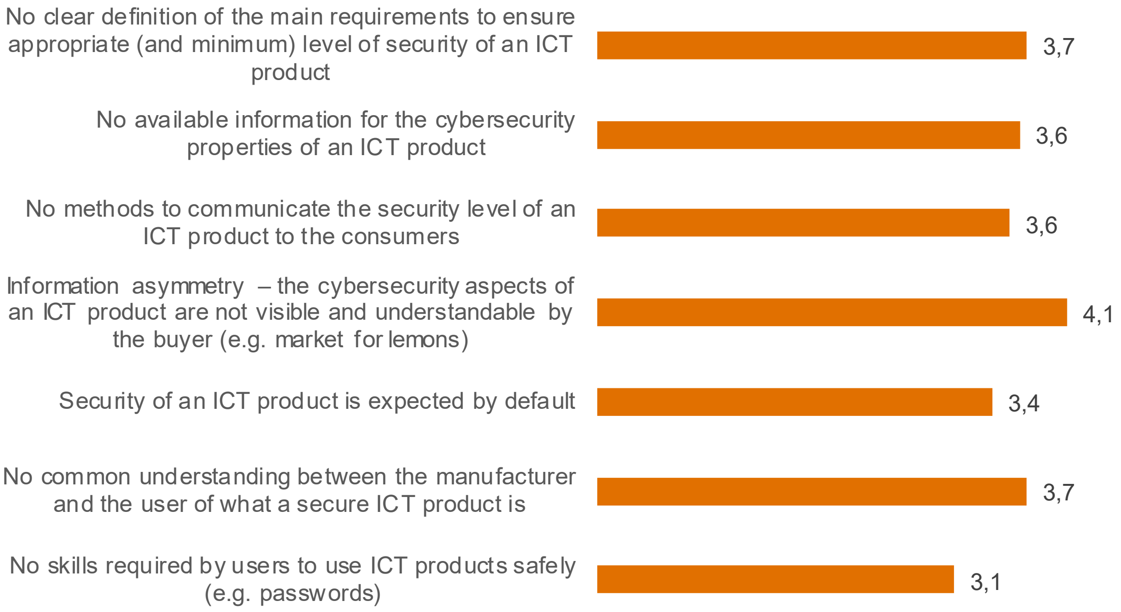
Figure 74 Q4: In your opinion, what is the level of understanding (awareness) among regular users (citizens) concerning the level of security of ICT products? (1-Poor; 2-Fair; 3-Good; 4-Very good; 5-Excellent)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Respondents somewhat agreed that the **biggest reasons for insufficient understanding among professional users** were information asymmetry – the cybersecurity aspects of an ICT product are not visible and understandable by the buyer (e.g. market for lemons), no clear definition of the main requirements to ensure appropriate (and minimum) level of security of an ICT product, and no common understanding between the manufacturer and the user of what a secure ICT product is (Figure 75). There were no significant differences between respondent types.

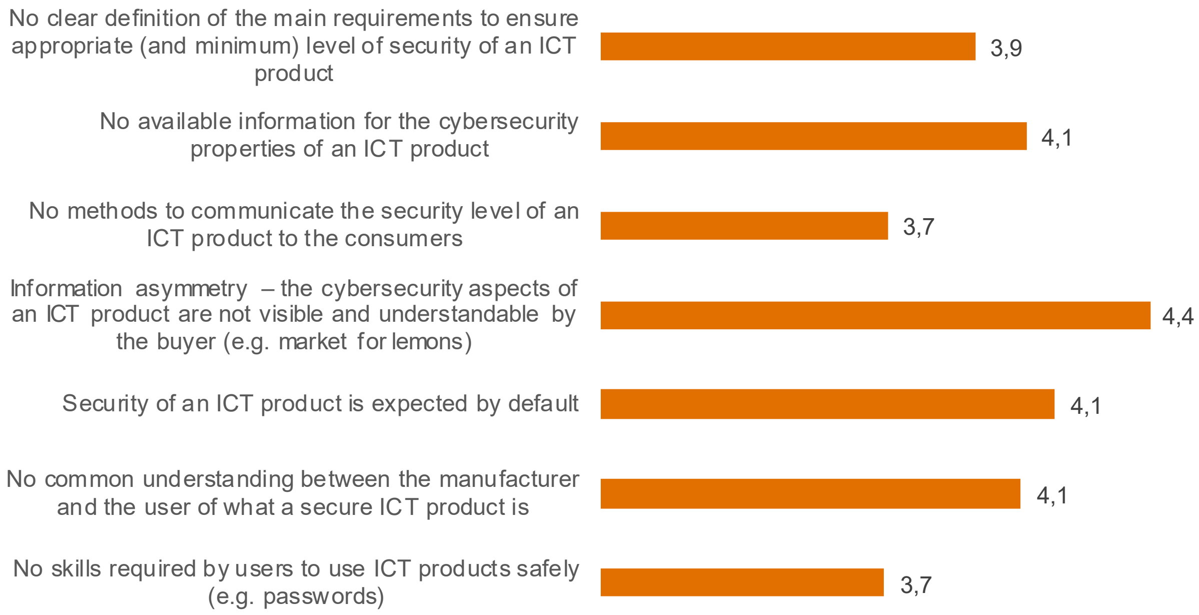
Figure 75 Q5: To what extent are the following statements a reason for insufficient understanding (lack of awareness/misperception) of the level of cybersecurity for ICT products among professional users? (1-Strongly disagree; 2-Somewhat disagree; 3-Neither agree



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Respondents somewhat agreed that the **biggest reasons for insufficient understanding among regular users (citizens)** were information asymmetry, no available information for the cybersecurity properties of an ICT product, no common understanding between the manufacturer and the used of what is a secure ICT product and that the security of an ICT product is expected by default (Figure 76). There were no significant differences between respondent types.

Figure 76 Q6: To what extent are the following statements a reason for insufficient understanding (lack of awareness/misperception) of the level of cybersecurity for ICT products among regular users (citizens)? (1-Strongly disagree; 2-Somewhat disagree; 3-Neither



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

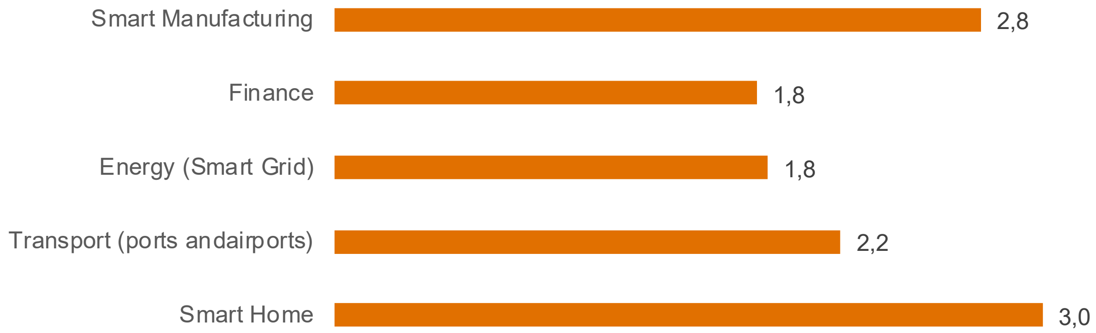
Cybersecurity issues as per ICT product categories and risk profiles

This section covers the questions seeking respondents' views on differences in cybersecurity risks according to ICT product types and their respective risk profiles.

Cybersecurity threats by sector

Respondents were asked to compare **five sectors covered by the study and rank them in terms of how severe cybersecurity threats they faced** (Figure 77). Respondents thought that Finance and Energy (Smart Grid) faced the highest threats, followed by Transport (ports and airports), Smart Manufacturing and Smart Home. There were no significant differences between respondent types.

Figure 77 Q7: Considering that an increasing number of products become smart/connected/IoT, please compare the five sectors covered by the study and rank them in terms of how severe cybersecurity threats they are currently facing (1-Highest threat; 5-Lowest threat)



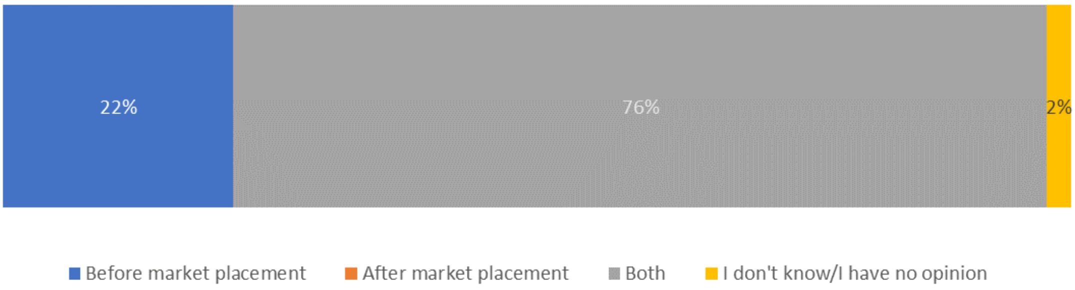
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Cybersecurity requirements for identified profile risks

Essential Requirements are security requirements designed to be applied to ICT products throughout their lifecycle. The study identified eight specific essential requirements from the first one covering product design to the eighth one covering continuous evaluation of and improvement to products' security.

Respondents were asked in which phases of an ICT product's lifecycle essential requirements should generally apply, distinguishing between pre-market placement and post-market placement.

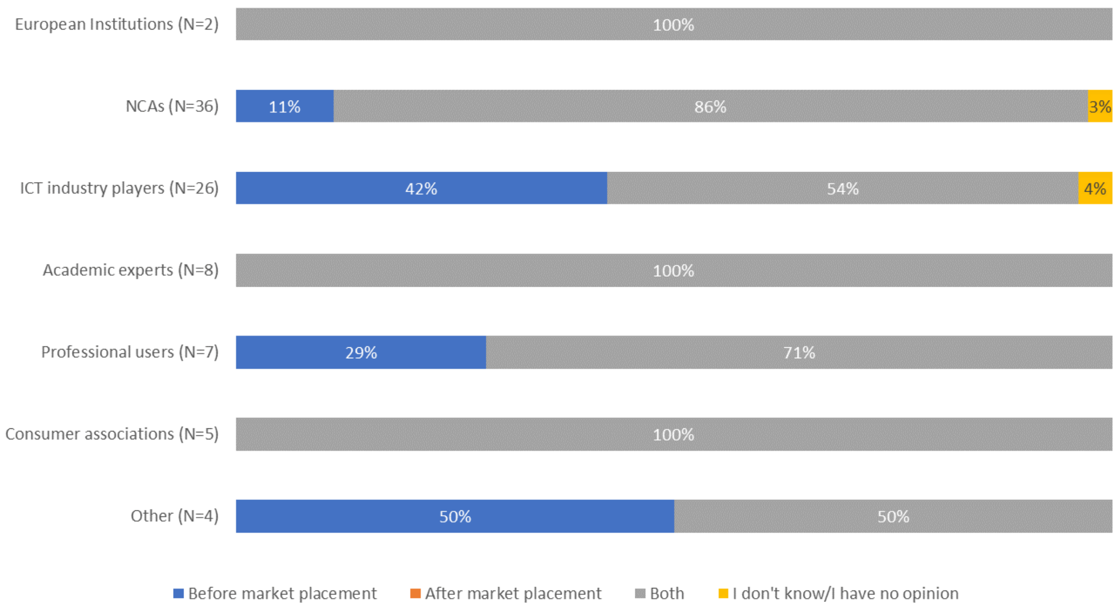
Figure 78 Q8: In your opinion, what phase(s) of the ICT product lifecycle should the Essential Requirements target?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Overall, just over three-quarters of the respondents thought that Essential Requirements should target ICT products before and after market placement while 22% indicated they should only apply before market placement.

Figure 79 Q8: In your opinion, what phase(s) of the ICT product lifecycle should the Essential Requirements target? (by stakeholder group)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Across the stakeholder groups, 42% of respondents on behalf of the ICT industry and 29% on behalf of professional users thought that Essential Requirements should only target ICT products before market placement (and 50% of 'other' respondents).

It was most frequently argued by these respondents that in the NLF, all Essential Requirements must be already met at the moment of placing a product on the market. Another point made was that the secure development lifecycle (SDL) of products should be built into the Essential Requirements as it allows a comprehensive approach to cybersecurity during the development of the product prior to market placement.

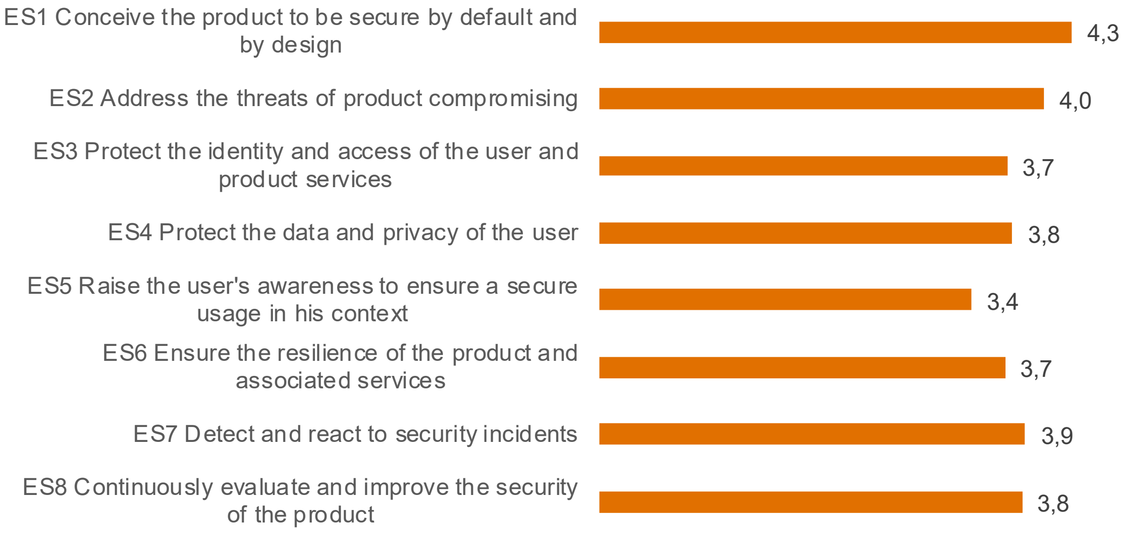
Across the different stakeholder groups, the most frequent point made in favour of having Essential Requirements apply before and after market placement was that cybersecurity is a dynamic phenomenon with a frequently changing cyber threat landscape requiring protection throughout ICT products' lifecycle, meaning before and after market placement.

Respondents were asked **to what extent the Essential Requirements address the main cybersecurity risks faced by ICT products** (Figure 80). Respondents gave the highest ratings to the following:

1. conceive the product to be secure by default and by design (ES1),
2. address the threats of product compromising (ES2)
3. detect and react to security incidents (ES7).

The least effective in terms of addressing the main cybersecurity threats was the essential requirement to raise the user's awareness to ensure a secure usage in his/her context (ES5)

Figure 80 Q9: To what extent do Essential Requirements listed above address the main cybersecurity risks faced by ICT products? (1-Do not address the main cybersecurity risks; 5-Address completely the main cybersecurity risks)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Several ICT industry players provided the following comments:

1. For a horizontal legislation ES should focus on properties verifiable for the product at the moment at placing on the market. ES1 and ES2 cover ES3, 4, 5 and 6. ES7 and 8 should be addressed either by processes in place (would be then part of ES1 and 2) or by obligations to economic operators.
2. ES2 is more reactive than proactive. ES3 and ES4 partially address the main cybersecurity risks. Regarding ES5, security should not depend on end users. ES6 requirement is not about resisting against attacks/threats but rather maintaining (or resuming) operation under (or after) an attack, even in degraded mode; it is more a mitigation/compensation than a protection mechanism. ES7 and ES8 are fundamental.
3. No essential requirement taken individually addresses completely the main cybersecurity risks, but they contribute together to security or compensation enforcement. They should be used together to ensure most effective approach.

Three NCAs had the following observations:

1. Main security risks are to be addressed by preventive measures: basic product design and specific features and their maintenance, that prevent unauthorized access to the device and its used cloud domain which can result in privacy violation and targeted fraud. Other measures are complementary, and related to life cycle management of the product, reducing impacts once attacks have taken place, and their contribution may therefore be slightly less.
2. Only a mix of these essential requirements can address completely the main cybersecurity risks.

3. These essential requirements are very generic and provide a good coverage of cybersecurity issues if interpreted accordantly. However, these requirements need specialization in order to form an effective regulation. Such a specialization should be undertaken during the development of European CSA certification schemes which allows to consider specific risk scenarios. Certain standards could be used to inform such a process, e.g. for consumer IoT products especially ETSI EN 303 645 specifies some of these essential requirements and is thus an important step in this direction.

Two consumer associations thought that a distinction should be made between technical and organisational requirements and that in conjunction the ES together address main cybersecurity risks.

One European institution commented that ES1 is definitively important but it may be difficult to practically implement it because cybersecurity threats continuously evolve, and it is difficult to anticipate all the future threats in the design phase. Still, it is an essential starting point.

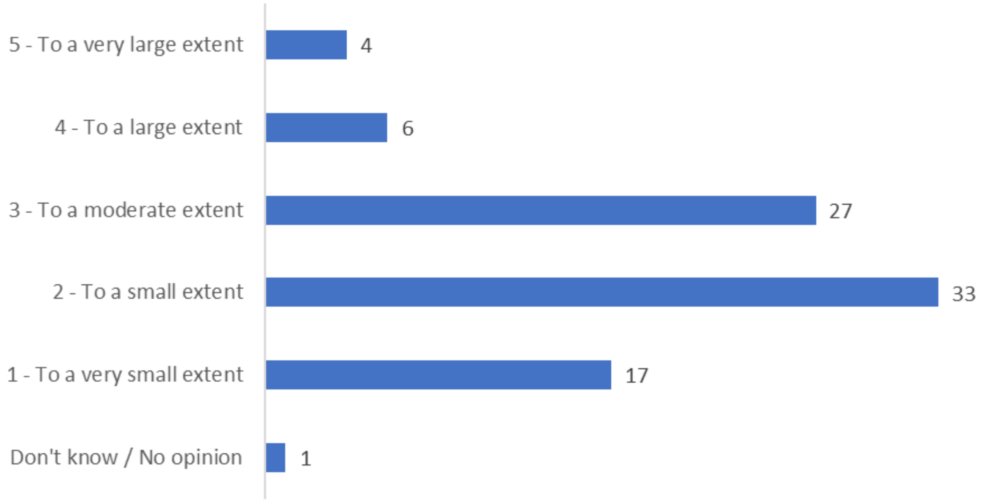
Proposed policy options for ICT cybersecurity

This section covers the questions asking respondents their views on the proposed options for future EU legislation on the cybersecurity of ICT products.

Policy option 1: Voluntary measures

The respondents were asked to rate as a policy option the extent to which the introduction of voluntary measures for the ICT industry would make ICT products cybersecure.

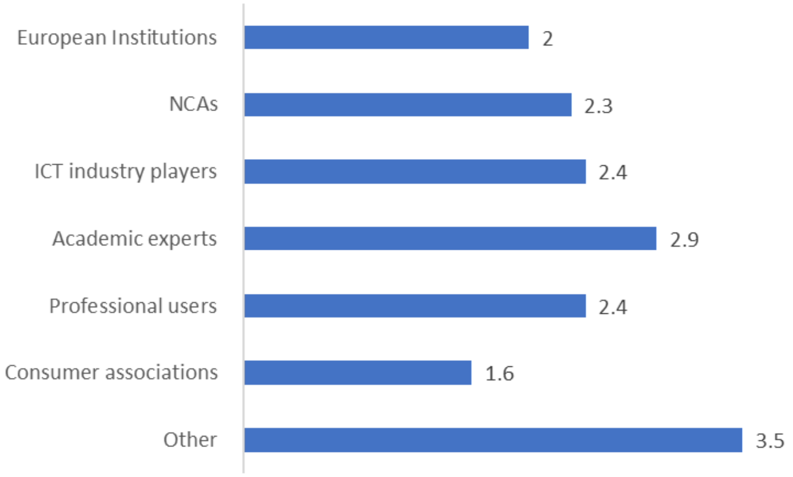
Figure 81 Q10: To what extent does the adoption of voluntary measures address the need of cybersecurity of ICT products?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Overall, this policy option was most frequently rated as addressing the need for cybersecure ICT products to **a small or very small extent**: 33 of the 88 respondents (37%) rated this policy option as addressing the issue to a small extent while 17 (19%) thought it did so to a very small extent. There were 27 respondents (31% of the total sample) who rated this policy option as addressing the need of cybersecure ICT products **to a moderate extent**.

Figure 82 Q10: Average rating of policy option 1 by stakeholder group (out of 5)



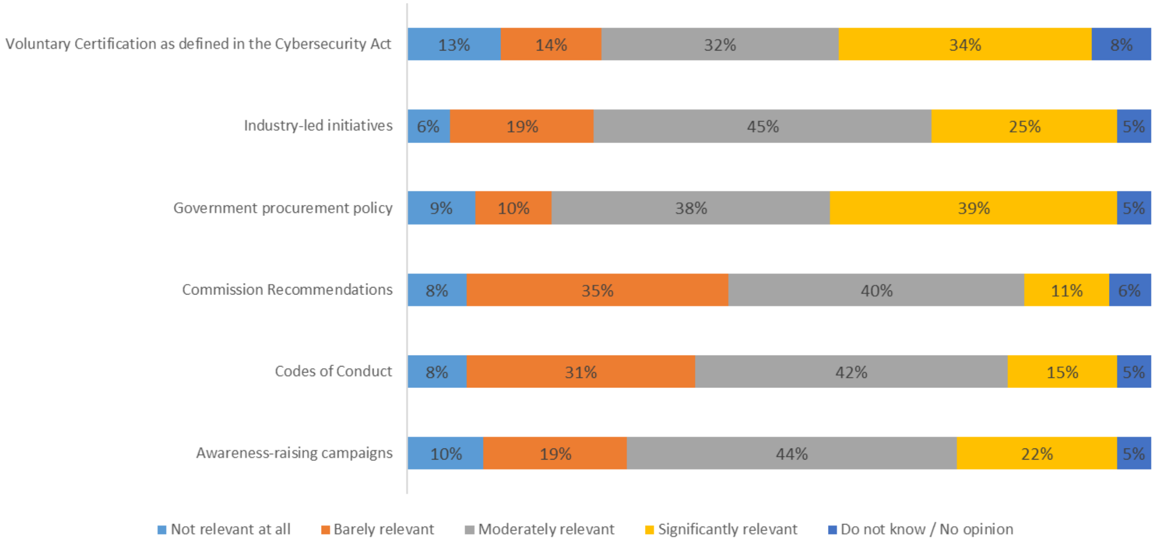
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Voluntary measures as a policy option received the lowest rating among consumer associations (N=5) but the highest rating among other respondents (N=4). Respondents across the stakeholder groups gave relatively similar ratings, judging this policy option addressing to a small extent the need for cyber secure ICT products.

The most frequent reason behind these ratings for NCAs and ICT industry players alike is that voluntary measures do not address market failures, that they are costly and therefore will not be taken up by most ICT industry players especially if there is no customer demand.

The respondents were then asked which measures under policy option 1 would be the most relevant to address the need for cybersecure ICT products.

Figure 83 Q11: Which of the following policy measures, envisaged under Policy Option 1- Voluntary Measures, is more relevant to address the need of cybersecurity for ICT products?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

The results above show that government procurement policies were judged as the most significantly relevant (by 39% of the respondents) compared to all others. Just over a third of the respondents (34%) judged that voluntary certifications as defined under the CSA would be the most significantly relevant.

A few respondents provided further explanations to support their answers to Q11. Among them, a respondent on behalf of the ICT industry indicated that while all the above measures were relevant, some additional ones could be considered such as: self-assessment, training of professional and end users, and exchange of best practices. Another respondent on behalf of the ICT industry indicated that all the above measures were relevant for establishing the right culture in the market and improve the reputation not only of companies that adhere to the standards, but also of governments that reach maturity in regulating the market.

Conversely, a respondent on behalf of an NCA commented that voluntary measures are generally not sufficient to ensure compliance with minimum security requirements established for all ICT products placed on the market.

As part of **Q12**, respondents were asked to **explain the possible effects, either positive or negative, that would stem from the implementation of voluntary measures**.

Both respondents on behalf of European institutions provided explanations in this regard:

1. A point made was that voluntary measures are not directly antagonised by the industry as they can give companies a head start to improve the cybersecurity of ICT product although voluntary measures can fail to effect changes if there is no market demand for improved cybersecurity.
2. Likewise, it was pointed out that while security conscientious vendors will try to design the best products for their customers, the latter often lack information to compare the security attributes of different ICT products which can lead to unfair competition where price is favoured to the detriment of security.

Several NCAs provided explanations on the likely positive and negative effects of the introduction of voluntary measures. There was consensus among the NCAs that voluntary measures would be too resource constraining to be taken up by most ICT companies, especially the smaller ones. As such, voluntary measures would not be sufficiently conducive to more secure ICT products overall.

Similar views were echoed among the respondents on behalf of the ICT industry who provided supporting explanations:

1. Voluntary measures tend to favour ICT companies who are large enough to implement through processes on security and which can communicate effectively on them; they would most likely lead to an industry status quo and not necessarily act effectively on improving security overall.
2. From a market perspective, security certifications are only relevant if customers ask for them. As such, it is unlikely that manufacturers and especially importers will make significant efforts on a voluntary basis due to the high investments required.

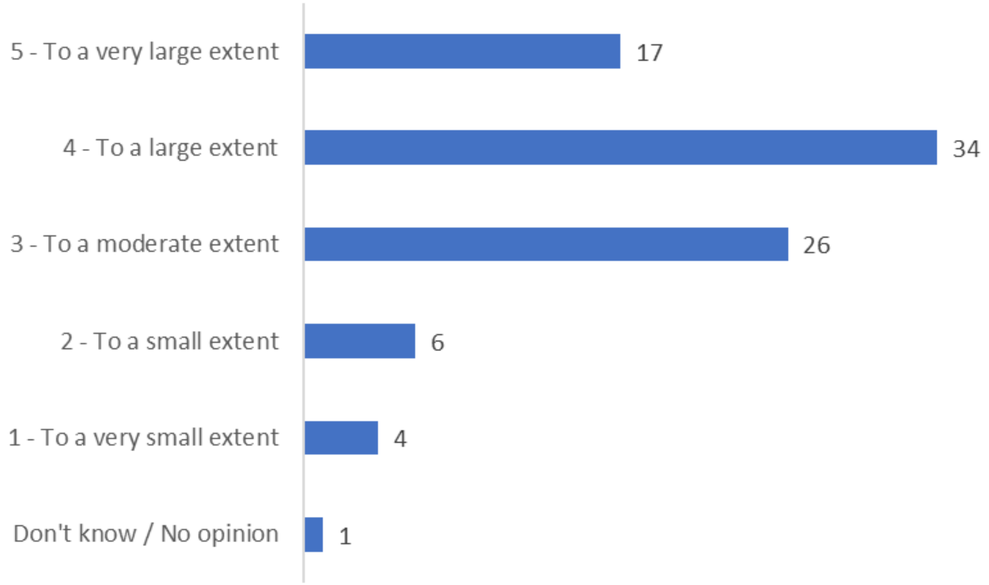
One consumer association explained that without proper mandatory regulation and requirements, manufacturers and retailers will prioritise short time to market, and profit margins over security and privacy. As such, voluntary measures do not incentivise meaningful actions to improve security.

Respondents on behalf of professional users and experts shared the view that voluntary measures would not lead to product standardisation and as such would be insufficient to ensure consistent security levels across the EU market.

Policy option 2: Horizontal legislation

The respondents were asked to rate as a policy option the extent to which the introduction of horizontal legislation would make ICT products cybersecure.

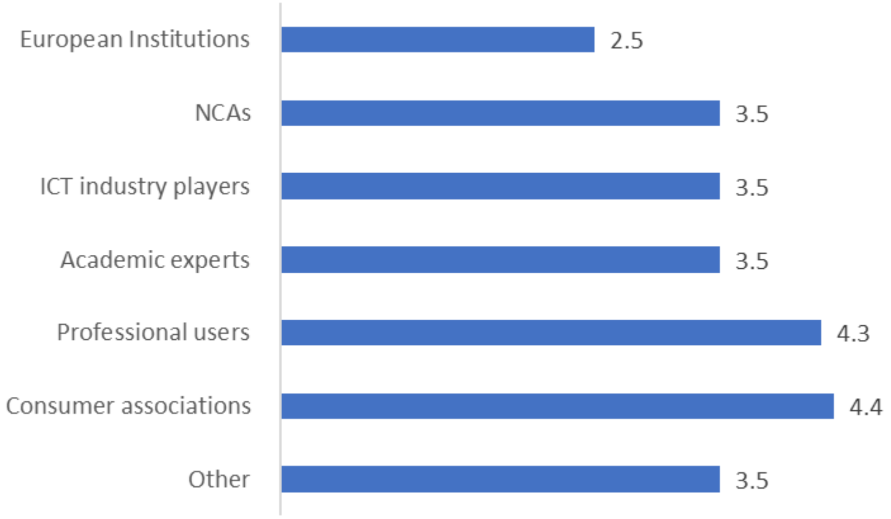
Figure 84 Q13: To what extent could the establishment of a horizontal legislation for ICT products and services address the need of cybersecurity of ICT products?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

This policy option was overall most frequently rated as addressing the need for cybersecure ICT products **to a large or a very large extent**: 34 of the 88 respondents (37%) rated this policy option as addressing the issue to a large extent while 17 (19%) thought it did so to a very large extent.

Figure 85 Average rating of policy option 2 by stakeholder group (out of 5)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Horizontal legislation as a policy option received the highest ratings among consumer associations (N=5) and representatives of professional users (N=7). The lowest rating (2.5 out of 5) was provided by respondents on behalf of EU institutions (N=2). Across the remaining groups, the average rating was 3.5 out of 5.

Various views were expressed to justify the ratings given across the different stakeholder groups.

Among NCAs judging that this policy option would not address the need for cybersecure ICT products, a frequent argument was that the existing EU Cybersecurity Act provides for a horizontal framework and simply needs to be better implemented. For ICT industry players judging the same, introducing horizontal legislation would not capture the differences in ICT products when it comes to cybersecurity and the legislation could become quickly outdated while reducing the effectiveness of CSA schemes.

Among those giving a moderate rating (3 out of 5), a frequent view expressed by NCAs and ICT industry players alike is that horizontal legislation would provide a good baseline, but this would need to be complemented with sector-specific legislation.

These views aside, most of the responding stakeholders made comments in favour of the introduction of horizontal legislation as an effective way to ensure cybersecurity for ICT products.

Among NCAs, the most frequent views were as follows:

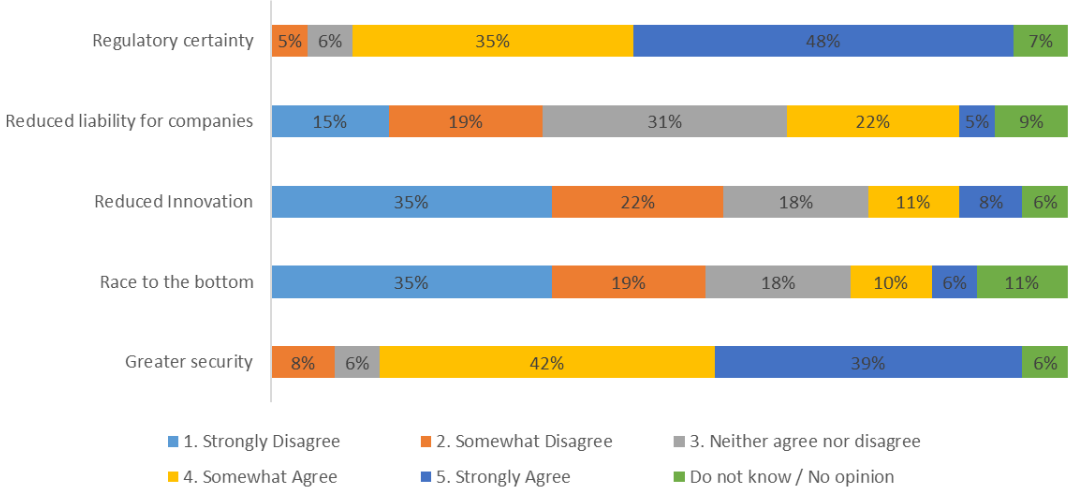
1. A new horizontal approach can fill gaps in existing legislation and provides for a mandatory security baseline for the EU common market while allowing for the inclusion of refinements based on Sector-specific risks.
2. Horizontal legislation is the most viable option to considerably raise the cybersecurity level of ICT products, as it will provide a clear legal framework, with principles and set of rules to follow for many products.

Among ICT industry players, the most frequent views were as follows:

1. Horizontal legislation creates more coherence and a level playing field along the value chain; it can define minimum security requirements applicable to all ICT products.

2. A horizontal approach will avoid the legal uncertainty caused by the currently developing patchwork of security requirements in several overlapping pieces of legislation. Furthermore, a horizonal approach could provide better support for other proposed legislative changes such as the NIS2.

Figure 86 Q14: To what extent do you agree with the following statements:
The horizontal legislation would result in:



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

A significant majority of the respondents agreed that the introduction of horizontal legislation would lead to regulatory certainty (83%) and enhance the security of ICT products (81%). Most respondents disagreed that this policy option would reduce innovation (57%) or cause a 'race to the bottom' (54%).

Some respondents commented on their answers to Q14 with the most recurrent positive observation in relation to policy option 2 being that it would harmonise minimum requirements, avoid market fragmentation in Europe as well as unfair competition.

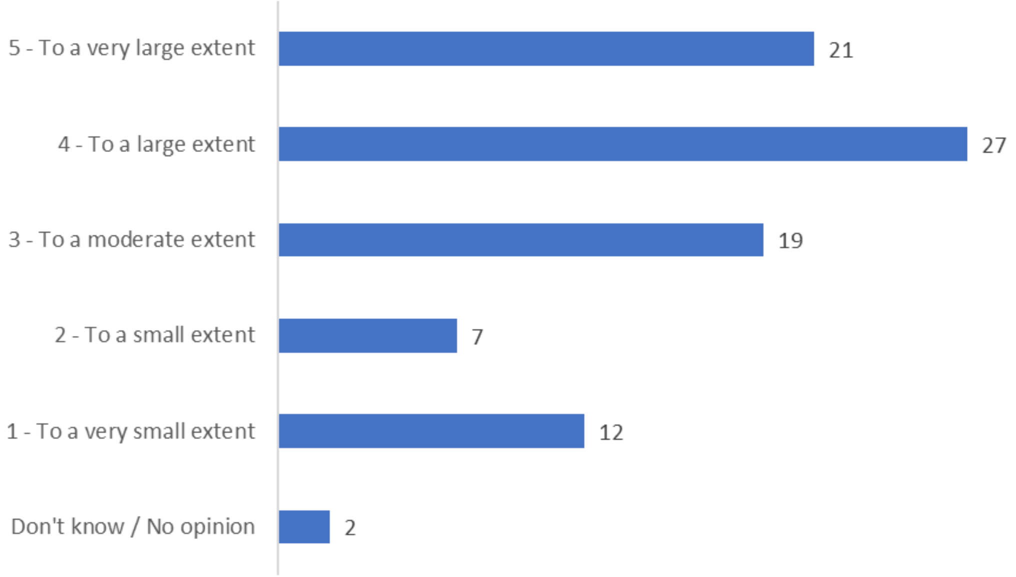
Some mixed observations were also made by a few respondents regarding policy option 2:

1. Two NCAs shared similar views that horizontal legislation will make it possible to set a generic rule without however precisely managing the requirements necessary for good protection, which means that complementary sector-specific regulations may be necessary. The reason given is that essential requirements may not be sufficiently forward-looking to ensure all ICT product types can be future proof given their specific risk profiles.
2. Echoing this view, one respondent on behalf of the ICT industry indicated that horizontal legislation should be complemented by additional requirements for products with higher risks.
3. Two consumer Associations argued that the adoption of a new horizontal cybersecurity law should be accompanied by the revision of the Product Liability Directive.

Policy option 3: Sector-specific legislation

The respondents were asked to rate as a policy option the extent to which the introduction of sector-specific legislation would make ICT products cybersecure.

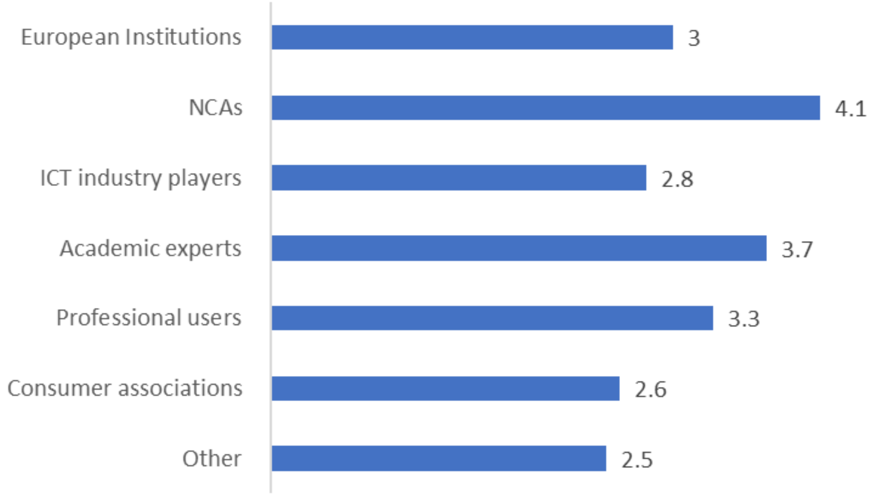
Figure 87 Q15: To what extent could the establishment of sector-specific legislation per sector address the need of cybersecurity of ICT products overall?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

This policy option was most frequently rated as addressing the need for cybersecure ICT products **to a large or a very large extent**: 27 of the 88 respondents (31%) rated this policy option as addressing the issue to a large extent while 21 (24%) thought it did so to a very large extent. The proportion of high ratings is very similar with policy option 2 (horizontal legislation). A relatively sizeable number of respondents (19 out of 88) thought this policy option only addressed the issue of cybersecurity to a small or very small extent.

Figure 88 Average rating of policy option 3 by stakeholder group (out of 5)



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

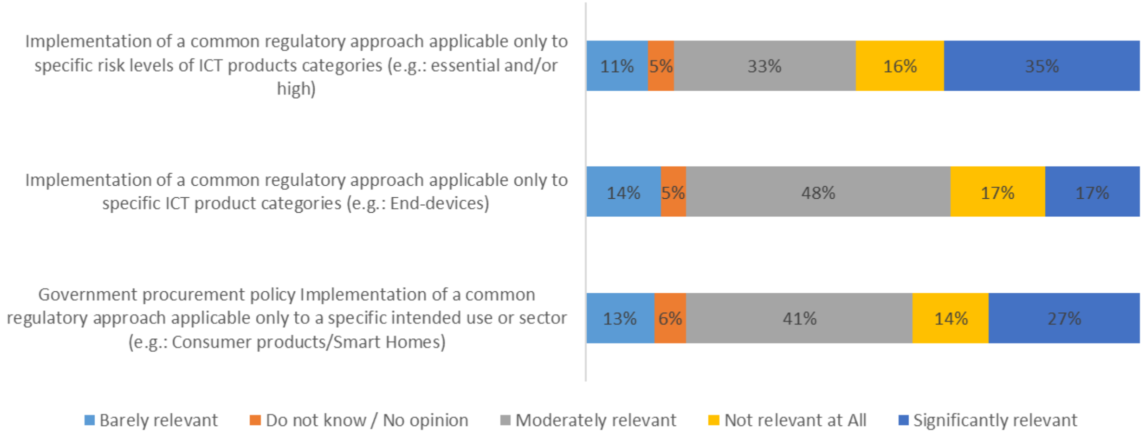
Sector-specific legislation as a policy option received the highest rating among NCAs (N=34; 2 respondents answered 'Do not know/No opinion). This must be contrasted with the lower ratings given among ICT industry players (N=26), consumer associations (N=5) and other stakeholders (N=4).

Among ICT industry players judging that this policy option would not address the need for cybersecure ICT products, a recurrent point made is that sector-specific legislation creates a complex legal architecture, with risk of market fragmentation, confusion and inconsistent or overlapping security requirements.

This view was echoed by two associations representing professional users. In addition, both these associations argued that sector-specific security requirements should not be part of legislation but should instead be left to widely accepted proven international standards to keep legislation technology neutral and account for differences across sectors.

NCAs in favour of this policy option often acknowledged the market fragmentation risks it poses but argued that sector-specific legislation should only cover the specific security needs of critical sectors while horizontal legislation should be the centrepiece addressing key cybersecurity issues.

Figure 89 Q16: Which of the following Sector-Specific Legislation types would be the most relevant to address the need of cybersecurity of ICT products?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Of the three types of sector-specific legislation put forward in Q16, the implementation of a common regulatory approach applicable to only specific risk levels of ICT product categories was deemed the most significantly relevant (35% of the respondents).

Several respondents provided explanations to support their answers to Q16 relating to sector-specific legislative approaches.

One respondent on behalf of the ICT industry and one respondent on behalf of professional users shared the view that sector-specific requirements should be left to widely accepted proven international standards to keep legislation technology neutral and account for differences across sectors while it remains essential to allow for a differentiated approach beyond a common baseline.

Two respondents on behalf of the ICT industry made the following observations:

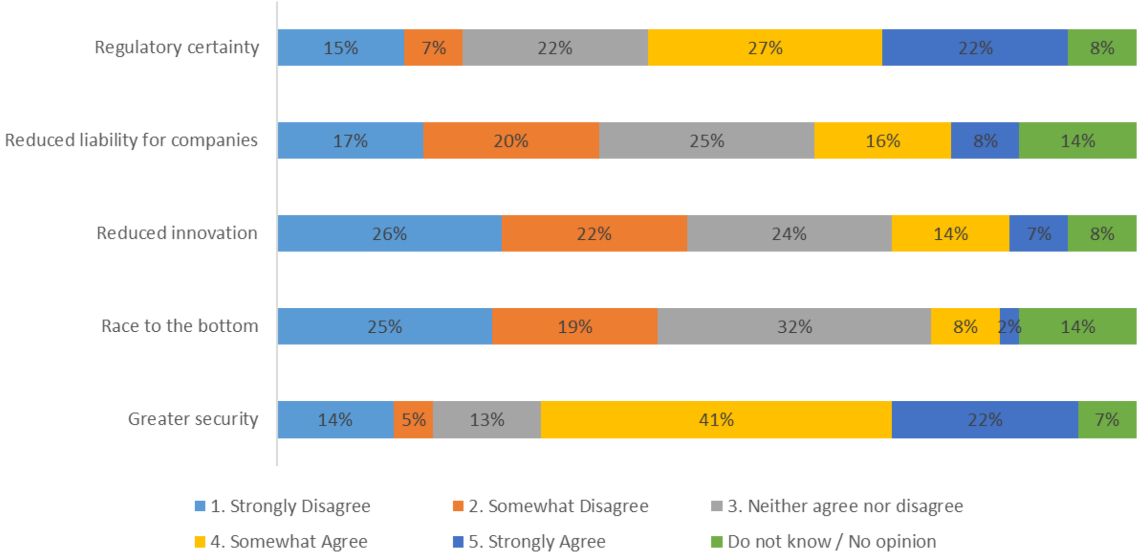
1. Addressing cybersecurity requirements based on risk level is common practice and most effective as low risk products do not need to have the same regulatory requirements as products with a higher risk level. However, some regulation is also needed for low-risk products.
2. Requirements should be handled through state-of-the-art, usually defined by using international standards, which will provide support for differences across sectors (e.g., ISO 27799 provides additional requirements to apply the security controls defined by ISO 27002 in the healthcare domain).

A few NCAs also provided supporting explanations which reveal some mixed views:

1. While sector-specific legislation implies the risk of fragmentation, it should only serve to supplement horizontal legislation and cover very specific requirements or risks for certain product types.
2. Sector-specific legislation should be used to make the schemes created under the Cybersecurity Act mandatory, clearly listing specific product categories and the various risk levels associated with each of them.

Lastly, one respondent on behalf of a European institution commented that sector-specific rules would end in continuous interpretations and revisions of their exact scope of applicability especially as ICT products and services increasingly overlap.

Figure 90 Q17: To what extent do you agree with the following statements:
the Sector-specific legislation of type 1 (implementation of a common regulatory approach applicable only to specific ICT product categories (Ex: end devices) would result in:



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Results were particularly mixed when respondents were asked to identify the likely effects of type 1 sector-specific legislation. Most of the respondents (63%) however agreed that type 1 sector-specific legislation would result in greater security for ICT products.

Respondents across stakeholder groups provided several comments:

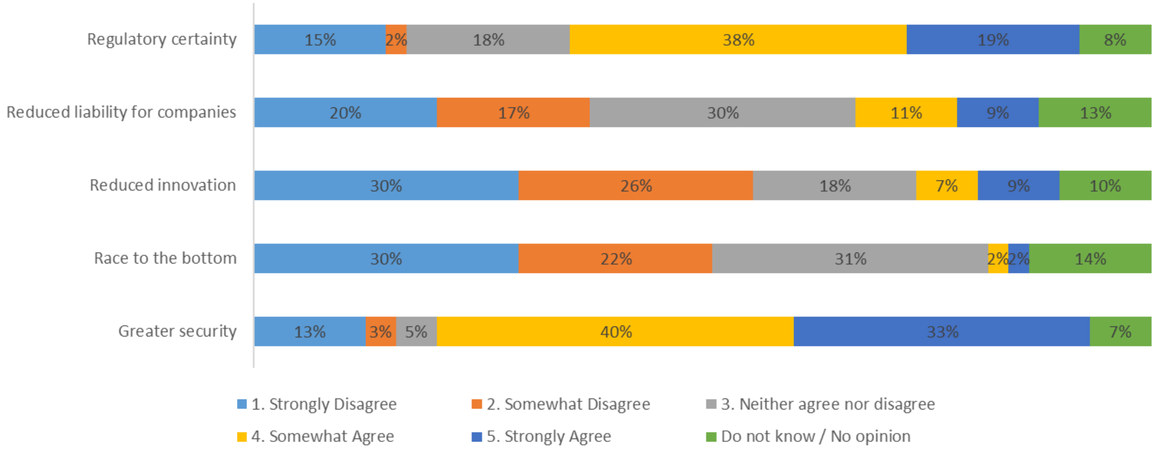
Several NCAs provided the following comments:

1. There is no need in making difference between the subcategories of the policy option 3 as product risk analysis is underlies all of these policy options. The (non) effect on innovation depends on the level technology-neutrality of the concerned legislation.
2. A focus on ICT categories of produce such as edge-based devices would be credible from a security perspective. Cybersecurity often focuses on access control provision with protecting digital assets.
3. There would be no reason to constantly improve security, once the product satisfies basic requirements.
4. Reduced liability for companies is not an intention of regulation in general.

ICT industry players provided the following comments:

1. Sector-specific legislation would be counterproductive. On the contrary, a horizontal legislation should be adopted, and widely accepted proven international standards should be left to keep legislation technology neutral and account for differences across sectors. Moreover, excessive legislation could lead to red tape, which can have a negative impact on cost and hence competitiveness.
2. Putting regulation in place to secure end devices might potentially increase costs for end-users as the low cost, often insecure devices are pushed out of the market. What is not clear from this proposal is how the regulation will tackle the end-to-end security. Most end devices do not exist on their own but are part of an integrated service. While the end device should obviously be secure to mitigate local issues, the integrated service might be a bigger concern.
3. While this approach has the merit of defining sectoral rules for specific end devices which are considered of higher security risk, introducing such legislation will inevitably lead to an increase in regulatory uncertainty and in potentially increasing liability for manufacturers. However, this remains the best approach under policy option 3.
4. Only devices in specific sectors would be improved.
5. Sectoral approach would be counterproductive. Conflicting and confusing regulations would fuel legal uncertainty, thereby hindering an effective and efficient addressing of cybersecurity, which also could lead to unforeseeable consequences for innovation and competitiveness in the area.
6. This provides ability to target regulations where they are needed.
7. Any regulatory requirement will lead to greater security. Companies will always be liable for their products, but a required independent conformity assessment move some of this liability to the third-party performing the assessment. The Project Team does not believe that the necessity of conformity reduces innovation. It will become just another checkbox a manufacturer has to check before going to the market. Furthermore, an innovative new product still needs to be secure.

Figure 91 Q18: To what extent do you agree with the following statements: *the Sector-specific legislation of type 2 (implementation of a common regulatory approach applicable only to specific risk levels of ICT products categories (Ex: essential and/or high risk)*



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

There were also mixed views when respondents were asked to identify the likely effects of type 1 sector-specific legislation. Most of the respondents however agreed that type 2 sector-specific legislation would result in greater security for ICT products (73%) and would improve regulatory certainty (57%).

Several NCAs provided comments:

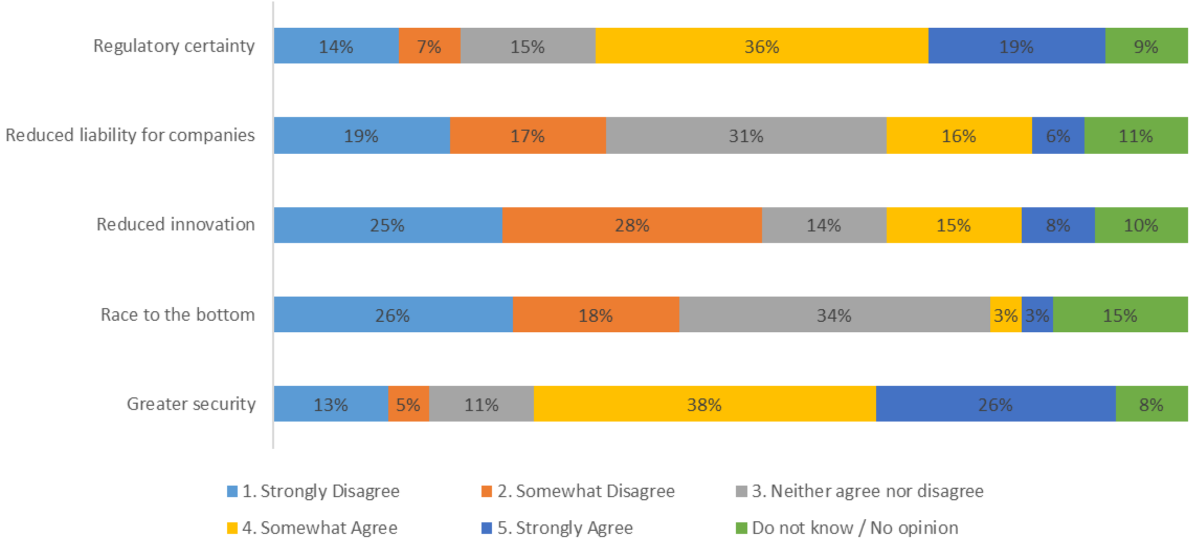
1. The question here is who ascertains the risk level. It is not possible to answer with this level of abstraction.
2. Risk-based approach is better understood and accepted by consumers, who expect greater security for "more important" things and for less important, they don't care much.
3. This approach requires proper risk assessment to be implementable.

ICT industry players had the following observations:

1. How does one compare risks over different sectors? Is it possible to create an assessment framework that normalizes risks over different types of products used in different sectors? Or does one foresee assessment frameworks per industry? Last but not least, is it possible to create a sensible risk assessment framework for cybersecurity?
2. The challenge with the identification of risk levels lies with the interpretation of competent authorities and/ or of conformity assessment methods to identify what constitutes an essential or high risk vs. lower-risk applications. It also creates duplication of compliance/ technical assessment regimes for products that are used across different risk levels.
3. It would be most challenging to define the risk level of products if they are used in different contexts.
4. Any regulatory requirement will lead to greater security. Companies will always be liable for their products, but a required independent conformity assessment would move some of this liability to the third-party performing the assessment. The Study Team does not believe that the necessity of conformity reduces

innovation. It will become just another checkbox a manufacturer has to check before going to the market. Furthermore, an innovative new product still needs to be secure.

Figure 92 Q19: To what extent do you agree with the following statements: *the Sector-specific legislation of type 3 (Implementation of a common regulatory approach applicable only to a specific intended use or sector (Ex: consumer products/smart Homes) would result in;*



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Like with type 2 sector-specific measures, most of the respondents agreed that type 3 sector-specific legislation would result in greater security for ICT products (64%) and would improve regulatory certainty (55%).

Several NCAs provided the following comments:

1. A specific intended use or sector makes sense for policy intervention. A focus on securing Smart Home devices as part of the Green Deal would be credible.
2. The easiest way to satisfy cybersecurity requirements, but there are so many specific categories for 'intended use' and legislators would have hard time to regulate them all.

ICT industry players made the following observations:

1. When focusing on the intended use, end-to-end security is in scope. I feel this approach would potentially result in the best result to increase cybersecurity across the border. It also allows focusing on the use case. For example, cybersecurity related to toys will have different points of attention than cybersecurity requirements related to smart homes.
2. Some technologies may become subject to multiple assessment procedures due to the intended use of the specific product (i.e. operating systems used for equally well for the operation of desktop PCs, as they are for running ATMs and nuclear submarines). This will lead to lesser regulatory certainty and it could potentially increase liability of producers/traders.
3. There are too many differences across sectors, and some could be so high risk that regulation may be necessary. Voluntary measures could lead to status-quo, horizontal approach is too strict for certain sectors

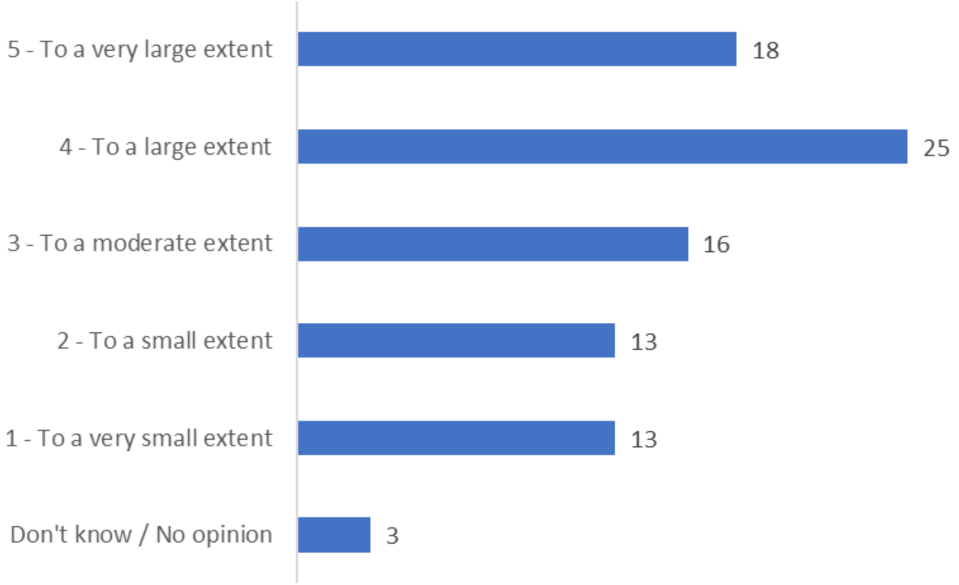
and not enough for high-risk sectors, and a mixed regulator approach is likely unmanageable effectively and could lead to further fragmentation. So, Policy Option 3 is the most adequate option with a combination of Type 2 and 3.

4. The concept of "intended use" is different and not interchangeable to the identification of a sector. The intended use is mostly dependent from the product, not the sector and often is in the B2B-context also addressed in the contractual relation. It could as vary in the same product category and even product family.
5. This has similar issues as the horizontal legislation approach - it is too broad and does not focus on high-risk products if the sectors are too broadly defined.
6. Intendent use and risk are to some extent related. However, even in the same intended use categories risk levels can greatly differ which might then lead to different requirements. However, any regulatory requirement will lead to greater security.

Policy option 4: Mixed approach (regulatory + voluntary measures)

The respondents were asked to rate as a policy option the extent to which the introduction of a mixed approach would make ICT products cybersecure.

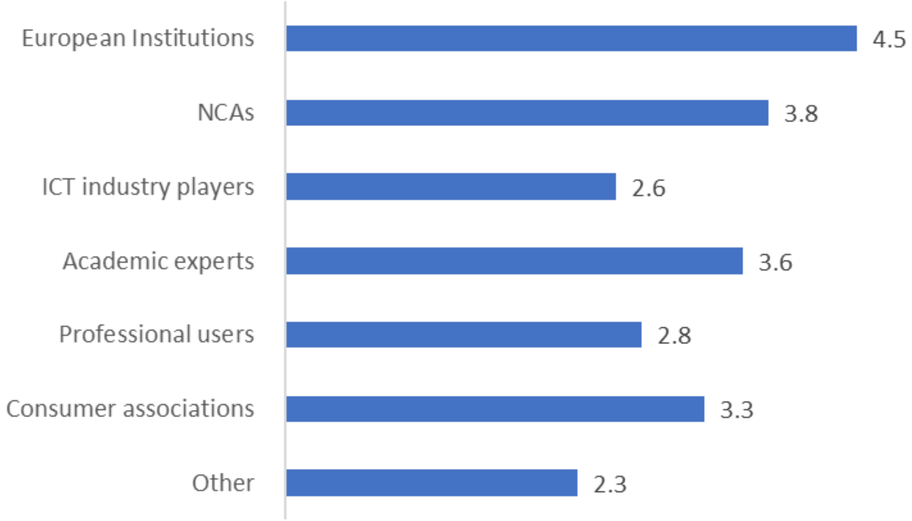
Figure 93 Q20: To what extent could the establishment of a Mixed Approach address the need of cybersecurity of ICT products?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Results show a split in the ratings with just under half of the respondents (43 out of 88) judging this policy option as addressing the need for cybersecure ICT products to a large or very large extent. However, almost a third of the respondents (26 out of 88) judged this policy option as addressing the need for ICT cybersecurity either to a small or very small extent.

Figure 94 Average rating of policy option 4 by stakeholder group (out of 5)



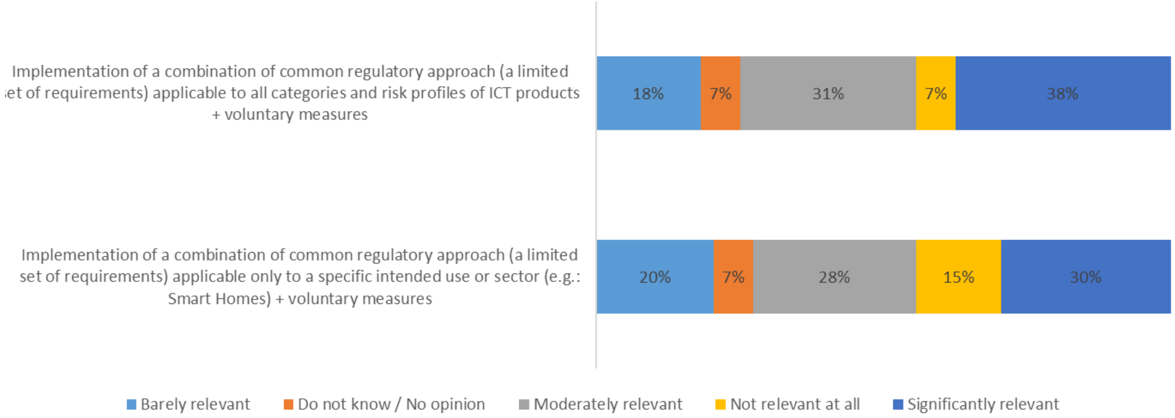
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

The average ratings by stakeholder group show a gap between European institutions (N=2) and NCAs (N=34; 2 respondents answered 'Do not know/No opinion) on the one hand and ICT industry players (N=26) and professional users on the other (N=7).

The most frequent argument shared by ICT industry players and professional users who judge this policy option as not addressing ICT cybersecurity effectively is that a mixed approach will only introduce more fragmentation in the ICT sector, greater legal uncertainty and confusion for both end-users and economic operators while failing to mitigate the risk of overlaps in legislation resulting in additional costs for everyone.

For NCAs and European institutions in favour of this policy option, a key point is that it would offer some flexibility in adaptation as different parts of the ICT market require a different approach due to varying levels of cybersecurity maturity. More specifically, a mixed approach would complement necessary regulation with voluntary measures to support market forces towards greater cybersecurity; an example given are the European CSA certification schemes which can provide in some sectors adequate frameworks to steer market forces or to harmonise national regulation across the EU.

Figure 95 Q21: To what extent would the following mixed approach types be relevant to address the need of cybersecurity of ICT products?



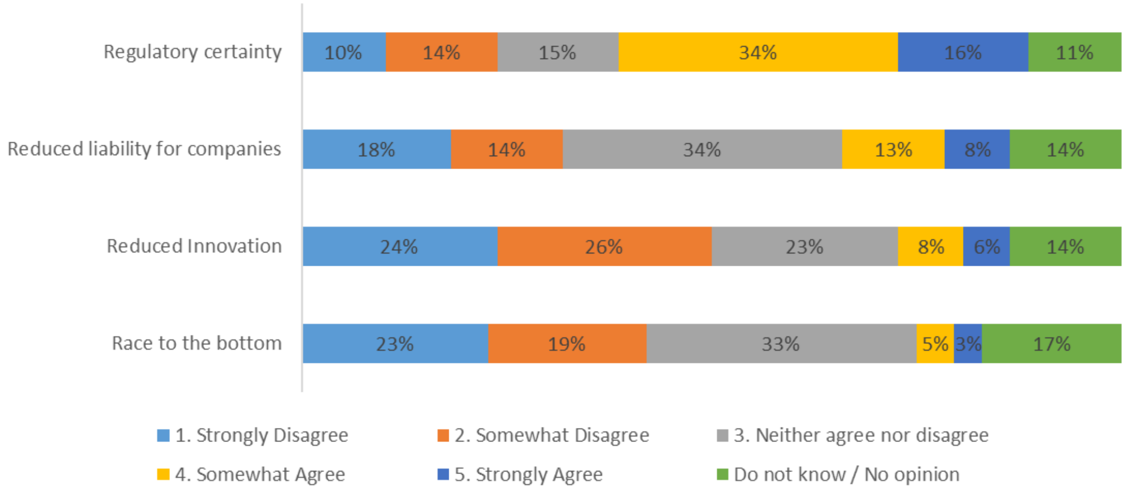
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Results show that for respondents, a mixed approach combining regulation applicable to all categories and risk profiles of ICT products and voluntary measures would be more significantly relevant than a mixed approach combining regulation applicable to specific ICT products and voluntary measures (38% vs. 30% of the total respondents).

Several respondents made remarks in relation to the relevance and effectiveness of types of mixed approaches. Criticisms were relatively often levelled at the mixed approach, notably among representatives of the ICT industry and of professional users. The most frequent criticisms were that a mixed approach may add unnecessary complexity, particularly when considering overlaps between different ICT products, and could create unfair competition among ICT sectors.

Among NCAs and European institutions, support for mixed approaches was marginally higher. It was argued that mixed approaches could be an effective response to the dynamic nature of ICT products, services and cyberthreats by including a set of more detailed and adaptable rules per sector, product category and associated risk level.

Figure 96 Q22: To what extent do you agree with the following statements: *the mixed approach of type 1 (implementation of a combination of regulatory and voluntary measures applicable to all categories and risk profiles of ICT products) would result in:*



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021). TARGETED CONSULTATION ONLINE SURVEY, N=88.

Just half of the respondents agreed that the mixed approach combining regulation applicable to all categories and risk profiles of ICT products and voluntary measures would result in regulatory certainty.

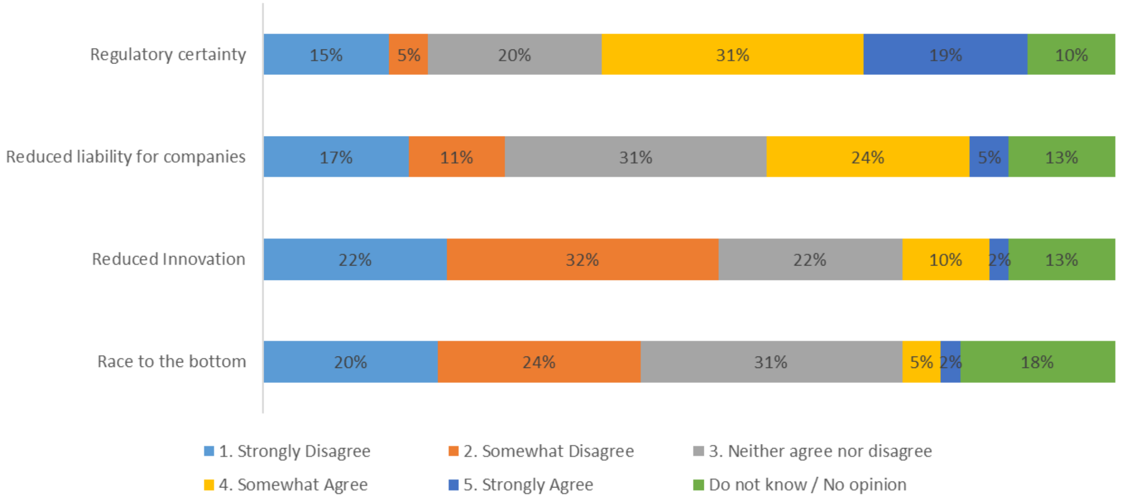
One professional user thought that this will result in additional costs for manufacturers due to the need to employ both experts on compliance and voluntary schemes.

Several NCAs thought that the beneficial impacts are less strong here than when sectoral regulation is (also) applied, and that this approach is too abstract to form a credible opinion.

ICT industry players made the following observations:

1. Voluntary measures do not work. If they did, then DDOS attacks would be a thing of the past through the deployment of BCP38. But no one wants to deploy it because of costs, and so we see an entire industry earning quite some money to protect companies from DDOS attacks when it could be solved by voluntary actions.
2. The common regulatory approach within a mixed approach type 1 might be the more favourable option, but it still would be subpar compared to a horizontal approach and it would also add unnecessary complexity, potential for confusion and potentially inefficiency.
3. This is type is too broad-based. It should be refined to address risk. One size does not fit all.
4. Additional costs for manufacturers due to the need to employ both experts on compliance and voluntary schemes.
5. A mixed approach may turn into the worst of kind of approach.

Figure 97 Q23: To what extent do you agree with the following statements*: the mixed approach of type 2 (implementation of a combination of regulatory and voluntary measures applicable only to a specific intended use or sector (Ex: Smart Homes) would result in:*



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Just half of the respondents agreed that the mixed approach combining regulation only applicable to certain ICT products and voluntary measures would result in regulatory certainty.

Two NCAs commented that the impacts desired are higher here but, again, they argued for a combined Sector-specific and horizontal approach (the latter with *lex specialis* clause because of the more specific sectoral legislation), and that fundamentally there should be core mandatory security requirements with flexibility for those who wish to go further with labels, codes of conduct etc. in a given sector.

Several ICT industry players provided the following comments:

1. Cybersecurity measures and requirements must be targeted at use cases/sectors, but the voluntary part is likely not to work.
2. As described previously, a sectoral approach would lead to incoherence, inconsistency, and fragmentation, which would be further worsened by yet another level of confusion through the addition of voluntary measures.
3. The preferred approach is horizontal legislation combined with specific regulations to address specific high-risk products.

Preferred policy option overall

The respondents were asked to indicate according to their views which of the four proposed policy options would best address the need for cybersecurity requirements for ICT products.

Table 99 Q24: Which of the proposed Policy Option would address better the need for cybersecurity requirements for ICT products?

Policy Option	No. of respondents	% respondents
0 – Baseline / No action	2	2%
1 – Voluntary measures	2	2%
2 – Horizontal legislation	25	28%
3 – Sector-specific legislation	24	27%
4 – Mixed approach	32	36%
Do not know / No opinion	3	3%

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Respondents were overall most likely to indicator that a mixed approach would best address the need for cybersecurity requirements for ICT products. Horizontal legislation is the second-best option according to the overall response.

Very few supporting comments were made by the respondents. Two comments were received in support of policy option 2 where it was argued that horizontal legislation would provide a high security baseline for all ICT products and could still accommodate vertical refinements through European CSA certification schemes to address Sector-specific risks.

One NCA went on to explain that a horizontal approach should have a clear hierarchy based on intended use, reducing the risk of legal uncertainty by following NLF elements such as conformity assessment (European CSA schemes) and market surveillance. Delegated acts may update the horizontal regulation with respect to new developments. In cases where a vertical refinement of regulation is not desired, a horizontal approach referencing the CSA would steer the market forces towards greater cybersecurity.

Impacts of the proposed policy options

This section relates to the impact assessment component of this study, seeking the views of the respondents on the likely impacts of each of the proposed policy options on the ICT industry but also professional and private users of ICT products.

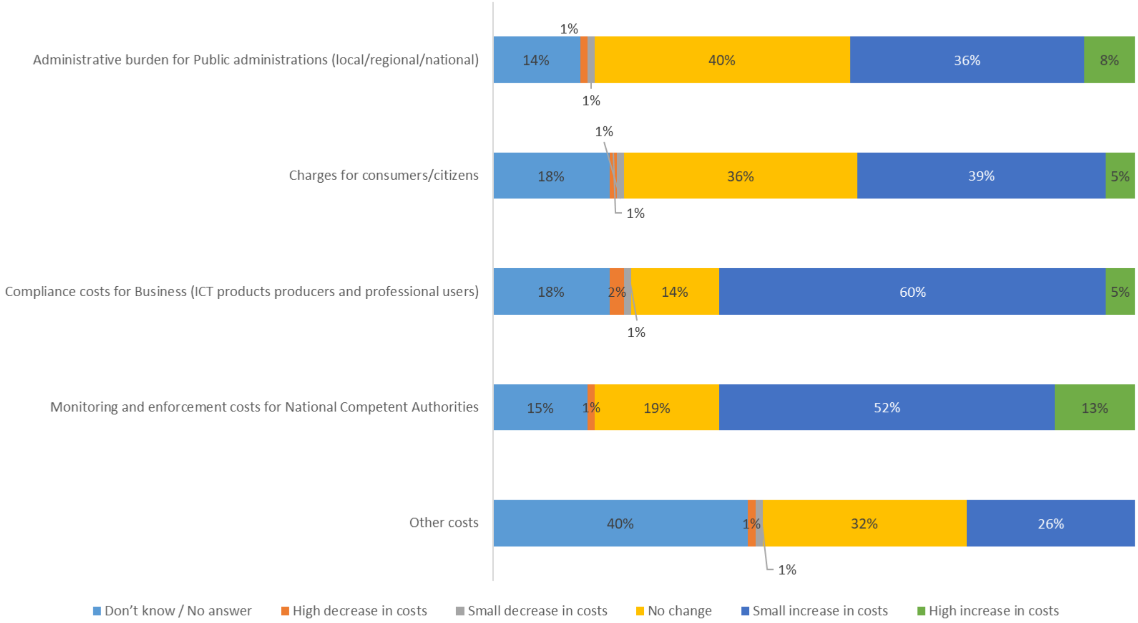
Impacts of the policy options on costs

The respondents were asked to identify what would be the impact of each of the four proposed policy options compared to no policy action on certain types of cost. These types of cost were listed as:

1. Administrative burden for Public administrations (local/regional/national)
2. Compliance costs for Business (ICT products producers and professional users)
3. Monitoring and enforcement costs for National Competent Authorities
4. Charges for consumers/citizens
5. Other costs

Where possible, the respondents were also asked to provide a quantification of these costs in FTE/EUR.

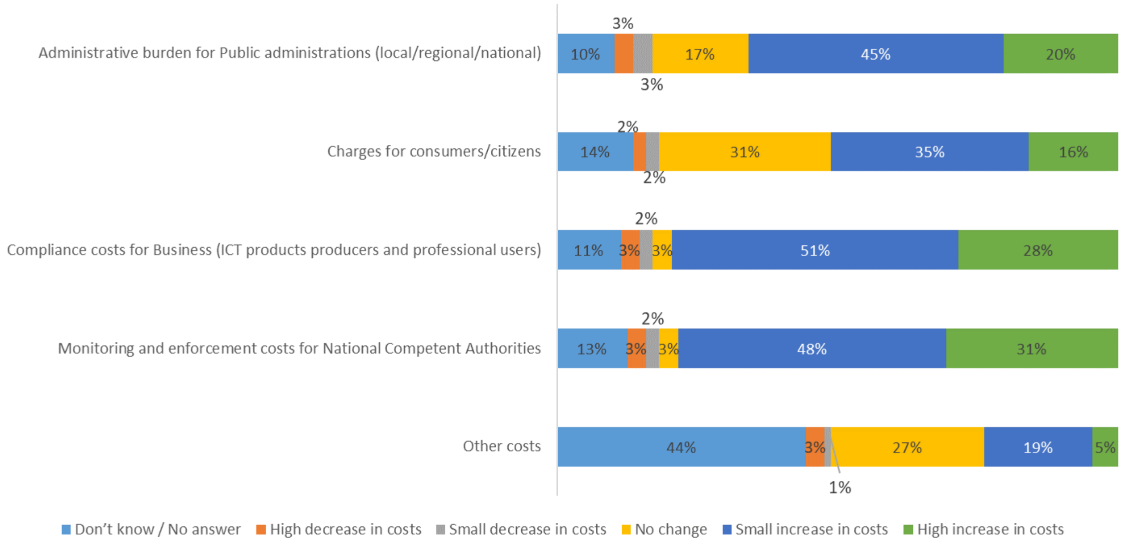
Figure 98 Q25: In your opinion, what would be the impact on costs of the Policy Option 1: Voluntary measures in comparison to no policy action?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

While respondents most frequently indicated that policy option 1 would result in a small increase in costs generally, especially compliance costs for ICT businesses (60% of all respondents), none of the respondents were able to provide a quantification of the costs linked to policy option 1.

Figure 99 Q26: In your opinion, what would be the impact on costs of the Policy Option 2: Horizontal legislation in comparison to no policy action?



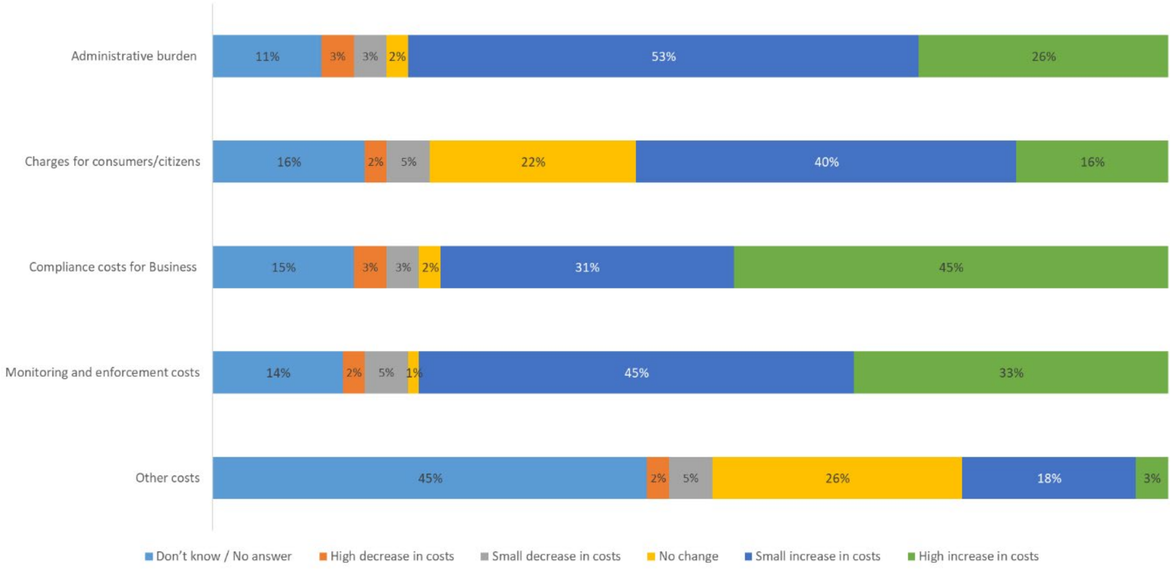
Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

Respondents indicated overall that the introduction of horizontal legislation would result in a small cost increase overall compared to no policy action: 51% of the respondents indicated that compliance costs for ICT businesses would slightly increase while a further 28% indicated that these would increase significantly. In addition, 48% of the respondents indicated that monitoring and enforcement costs for NCAs would increase slightly while a further 31% indicated that these would increase significantly.

A few respondents were able to provide a quantification of the costs linked to policy option 2.

1. A NCA specified that the costs of implementing this policy option would amount to an additional 6 FTE or EUR 1.6 million for public administrations.
2. For two respondents on behalf of the ICT industry, implementing this policy option would result in a 10-15% increase in costs generally. Another respondent on behalf of the ICT industry added that such additional costs would be much lower compared to having Sector-specific legislation or a mixed (i.e. horizontal and sector-specific) approach.
3. For a representative of professional users, additional costs were estimated at 5% but these would be compensated by savings made in addressing and managing cybersecurity risks.

Figure 100 Q27: In your opinion, what would be the impact on costs of the Policy Option 3: Sector-specific legislation in comparison to no policy action?



Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

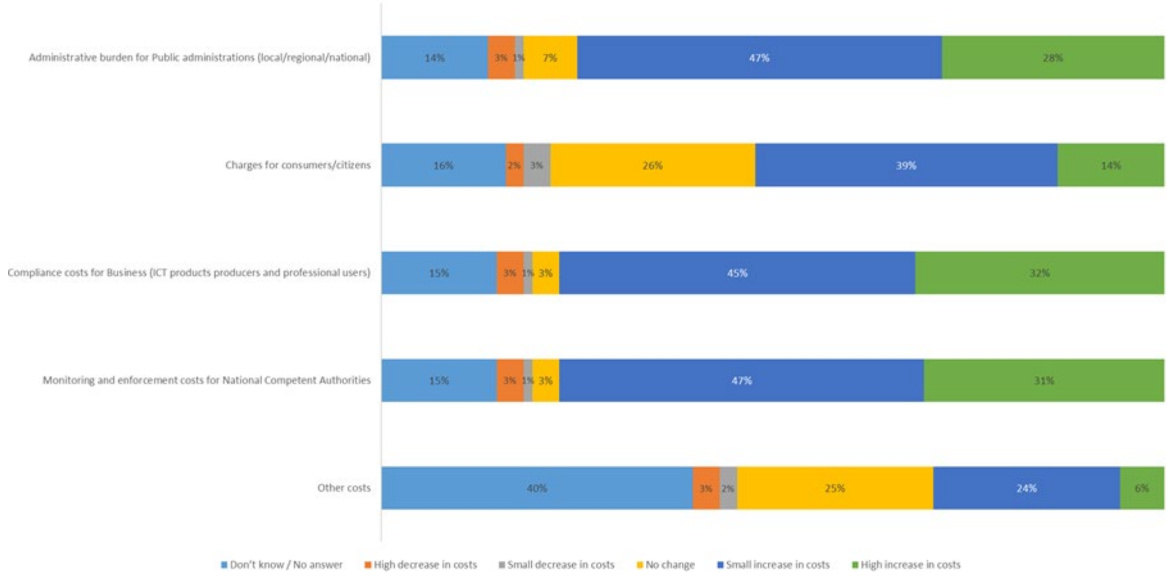
Respondents indicated overall that the introduction of sector-specific would result in small to significant cost increases overall compared to no policy action: 53% of the respondents indicated that the administrative burden for public authorities would would slightly increase while a further 26% indicated that these would increase significantly. In addition, 45% of the respondents indicated that compliance costs for ICT businesses would increase significantly while a further 31% indicated that these would increase slightly. Interestingly, 40% of the respondents indicated that policy option 3 would mean slightly higher prices for consumers with a further 16% indicated this would result in significantly higher consumer prices.

A few respondents were able to provide a quantification of the costs linked to policy option 3.

1. A NCA specified that the costs of implementing this policy option would amount to an additional 9 FTE or EUR 2 million for public administrations.
2. For three respondents on behalf of the ICT industry, implementing this policy option would result in a 15-20% increase in costs generally.

A frequent observation among respondents on behalf of the ICT industry was that fragmentation and overlapping regulation resulting from a sector-specific approach would increase compliance costs substantially.

Figure 101 Q28: In your opinion, what would be the impact on costs of the Policy Option 4: Mixed approach (regulatory + voluntary measures) in comparison to no policy action?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

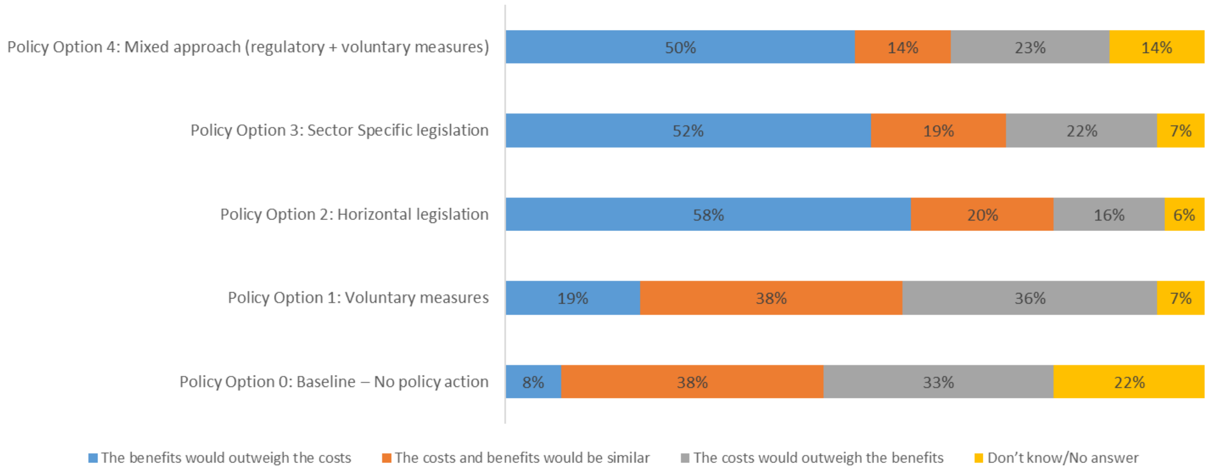
Overall, the mixed approach was deemed as resulting in small to significant cost increases compared to no policy action, but to an even greater extent than policy option 3 (sector-specific legislation). For 47% of the respondents, monitoring and enforcement costs for NCAs would increase slightly while these would increase significantly for a further 31%. Similarly, 47% of the respondents indicated that the administrative burden for public authorities would increase slightly with a further 28% indicating these would increase significantly. Most respondents (77%) also deemed that policy option 4 would increase compliance costs for ICT businesses either slightly or significantly.

Regarding cost quantification, An NCA specified that the costs of implementing this policy option would amount to an additional 14 FTE or EUR 3 million for public administrations.

A handful of respondents representing professional users argued that this policy option would result in additional costs from the need to employ experts both on regulatory compliance and on voluntary schemes.

In summary, the respondents were asked to rate the cost-effectiveness of each of the four policy options.

Figure 102 Q29: Please rate the cost-effectiveness of the policy options:



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Overall, horizontal legislation was deemed to be cost-effective by 58% of the respondents while policy option 3 was deemed to be cost-effective by 52% of the respondents and policy option 4 by 50% of the respondents. Respondents were most likely to indicate that the costs of policy option 1 (voluntary measures) would outweigh its benefits.

A few respondents made comments on cost-effectiveness, the most frequent ones suggested policy option 2 (horizontal legislation) to be the most cost-effective.

Five respondents on behalf of the ICT industry and one respondent on behalf of professional users shared the view that a horizontal cybersecurity product legislation, which can build on well-established and proven mechanisms for market access, is the best way forward to cost-effectively ensure product safety in the EU. For one consumer association, regulations concerning consumer safety should always be introduced as horizontal legislation.

Conversely, three respondents on behalf of the ICT industry thought that policy options 3 or 4 could potentially be more cost-effective than policy option 2. More specifically, sector-specific legislation would be potentially more cost-effective depending on how it is implemented and enforced. In this regard, it was suggested four generic sectors should each be covered in horizontal legislation (Consumer, Enterprise, Industrial, Critical) and vertically through voluntary schemes.

Wider impacts of the policy options

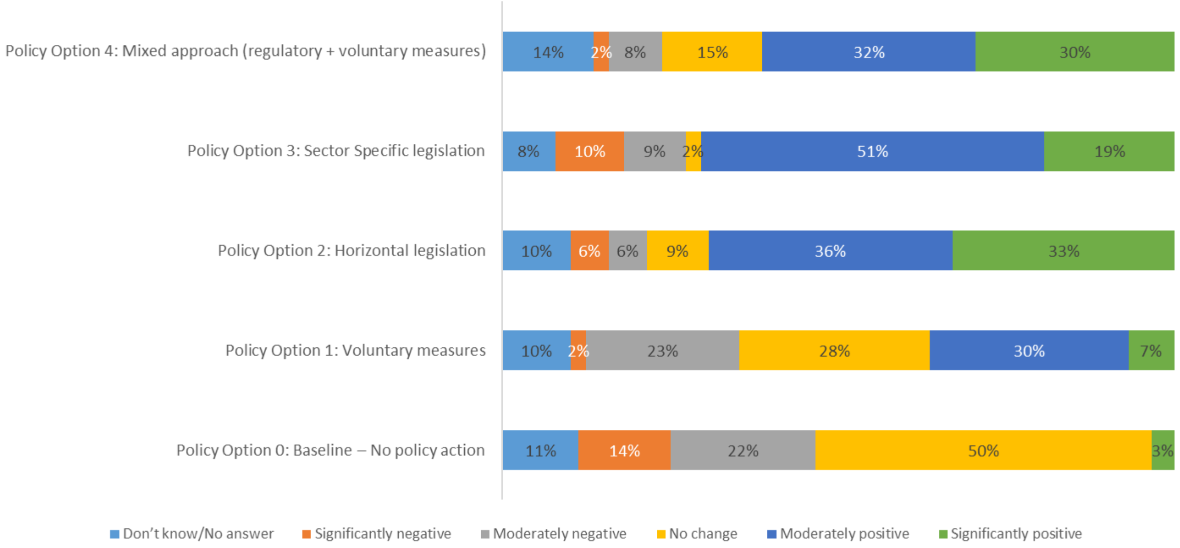
The respondents were also asked to assess the impact of each of the four proposed policy options on the following aspects:

1. Competitiveness of the EU's ICT industry on a global level
2. Innovation in the EU's ICT industry
3. Creation of a level playing field within the EU's ICT market
4. Availability of reliable and secure ICT products in the EU's internal market
5. Public trust in ICT products

6. Fundamental rights, especially in relation to consumer and data protection

The results are presented in the following charts.

Figure 103 Q30: What would be the overall impact of the policy options on the competitiveness of EU's ICT industry?



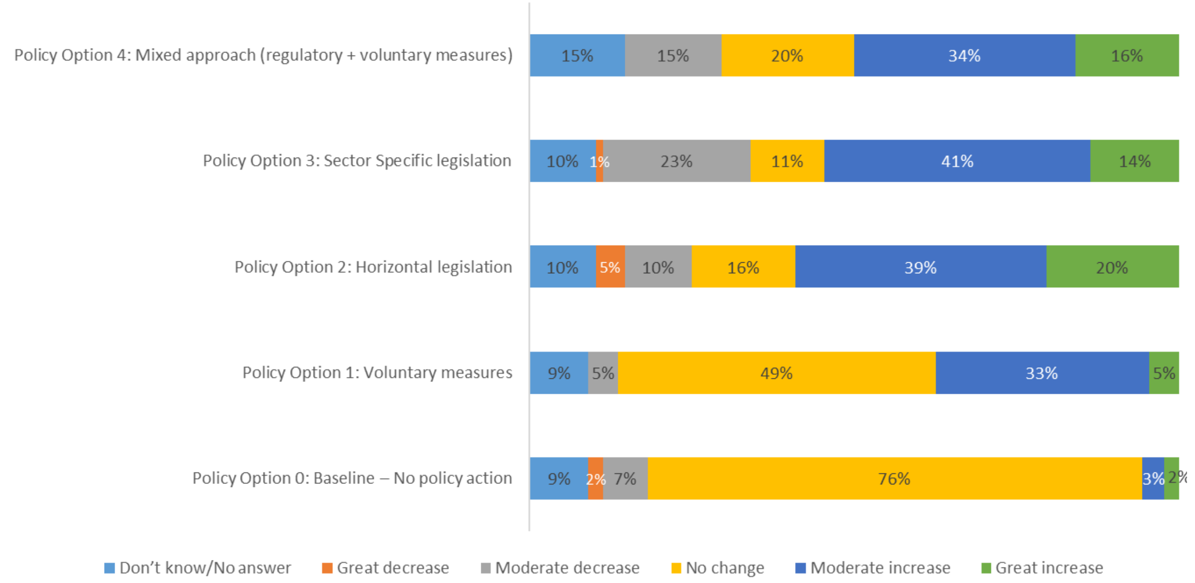
Source: Study on the need of Cybersecurity requirements for ICT products (2021), Targeted consultation online survey, N=88.

Of all the policy options, policy option 2 (horizontal legislation) was most frequently deemed to be likely to generate significantly positive impacts on the competitiveness of the EU's ICT industry (33% of all respondents), followed by policy option 4 (30% of all respondents. Policy option 3 (sector-specific legislation) was most frequently deemed likely to generate moderately positive impact on the competitiveness of the EU's ICT industry (51% of all respondents).

A few respondents commented on the policy options in relation to global competitiveness of the EU's ICT industry.

1. The most frequent point made, especially by respondents on behalf of the ICT industry and professional users, was that having uniform ICT security requirements across and beyond the European Digital Single Market though horizontal legislation will allow companies operating across the EU to manage risk in a cohesive manner, and therefore ensure EU competitiveness on a global level.
2. One respondent on behalf of the ICT industry acknowledged that if ICT security is not as relevant outside the EU market, then additional efforts made by the EU ICT industry will make its products more expensive but at the same time this will cause competitors with less secure products to either drop out of the global market or to adjust their products to higher security standards, which is ultimately a positive for the EU ICT industry.

Figure 104 Q31: What would be the overall impact of the policy options on the innovation in EU's ICT industry?



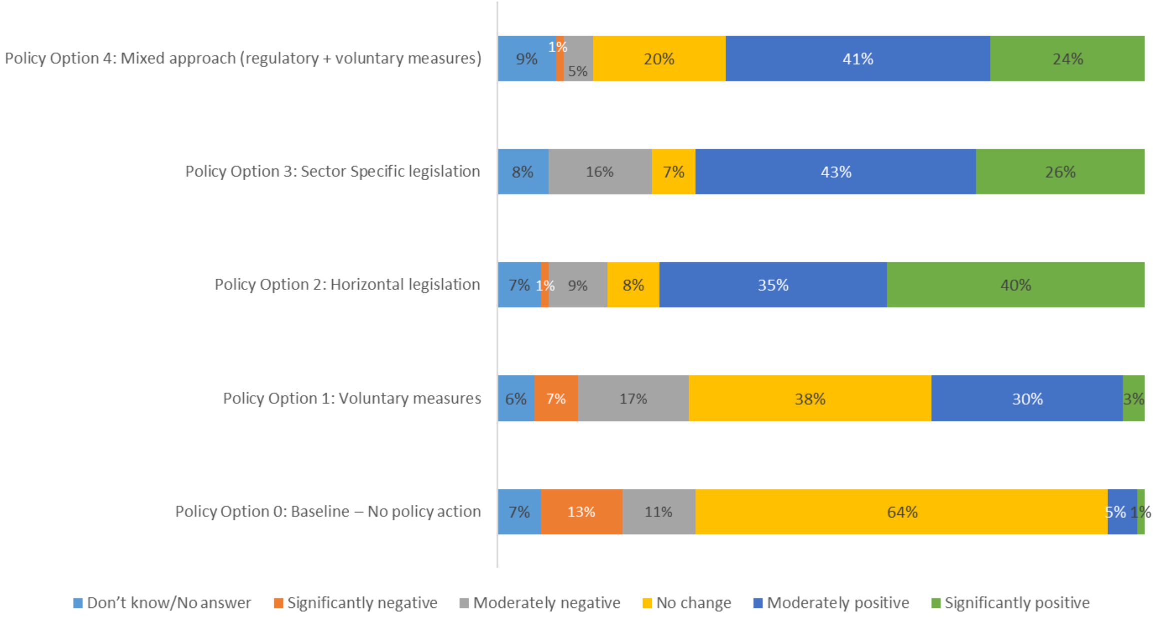
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Of all the policy options, policy option 2 (horizontal legislation) was most frequently deemed to be likely to generate significantly positive impacts on innovation in the EU's ICT industry (20% of all respondents). Policy option 3 (sector-specific legislation) was most frequently deemed likely to generate moderately positive impact on the innovation of the EU's ICT industry (41% of all respondents).

A few respondents commented on the policy options in relation to innovation within the EU's ICT industry. Views as to their potential in stimulating innovation overall were rather mixed.

1. For three respondents on behalf of the ICT industry, laws to improve security standards across the board will be conducive to innovation. Examples given were the development of new methodologies and technologies to make product security testing more efficient and reliable, and the development of secure platforms focused on the security requirements of products whereby businesses using the platform can focus on innovative applications.
2. For one NCA, the policy options around security certification could potentially drive innovation. For example, a compulsory conformity assessment under CSA based on a horizontal legislation could lead to innovations since potential vulnerabilities would be detected earlier and are better known. In addition, establishing product security profiles for certification creates a need for innovative solutions in specific product areas.
3. Conversely, three respondents on behalf of professional users held the view that security is not a driver of innovation unlike customer demand or functionality of ICT products. There is nevertheless the acknowledgment that ICT product security is also a component of customer demand and functionality.

Figure 105 Q32: What would be the overall impact of the policy options on fairness in competition in the EU's ICT market? (i.e. creating a level playing field within the EU's ICT market)

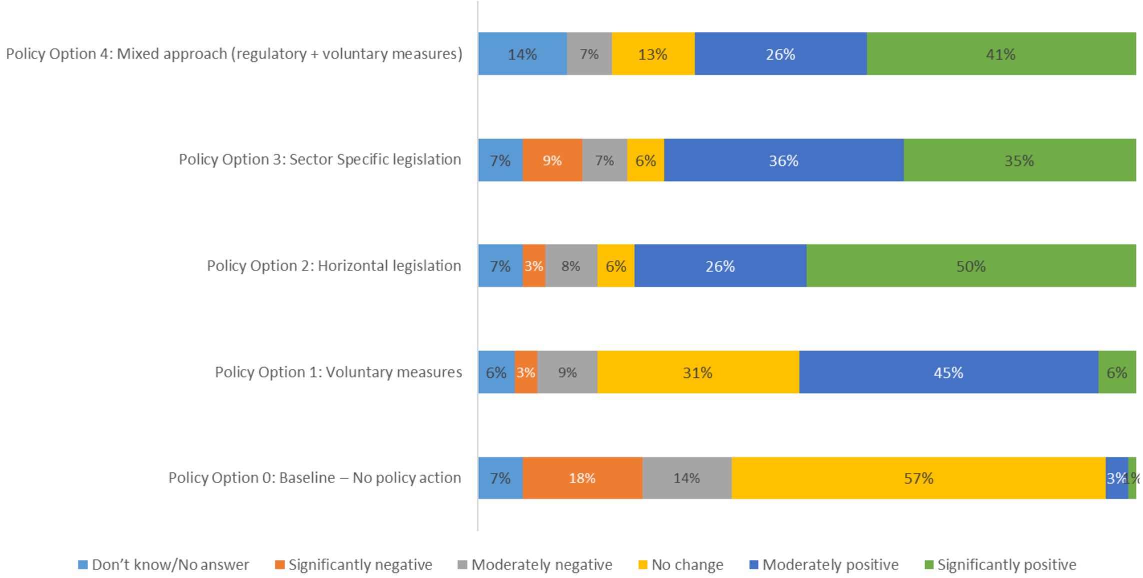


SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Policy option 2 (horizontal legislation) was much more frequently deemed as having a significantly positive impact on creating a level-playing field in the EU ICT market (40% of all respondents) compared to the other policy options. Only 26% of the respondents deemed policy option 3 (sector-specific legislation) would have a significantly positive impact on the EU ICT market and only 24% of the respondents thought the same about policy option 4 (mixed approach).

In relation to the level playing field aspect, one comment frequently came back among all respondent types but particularly ICT industry players in support of the introduction of horizontal legislation as it will address the fragmentation of the European cybersecurity landscape potentially resulting from specific national rules which threaten to undermine the competitive advantage of a European Digital Single Market without yielding meaningful security benefits.

Figure 106 Q33: What would be the impact of the policy options on the availability of reliable and secure ICT products in the Internal Market?

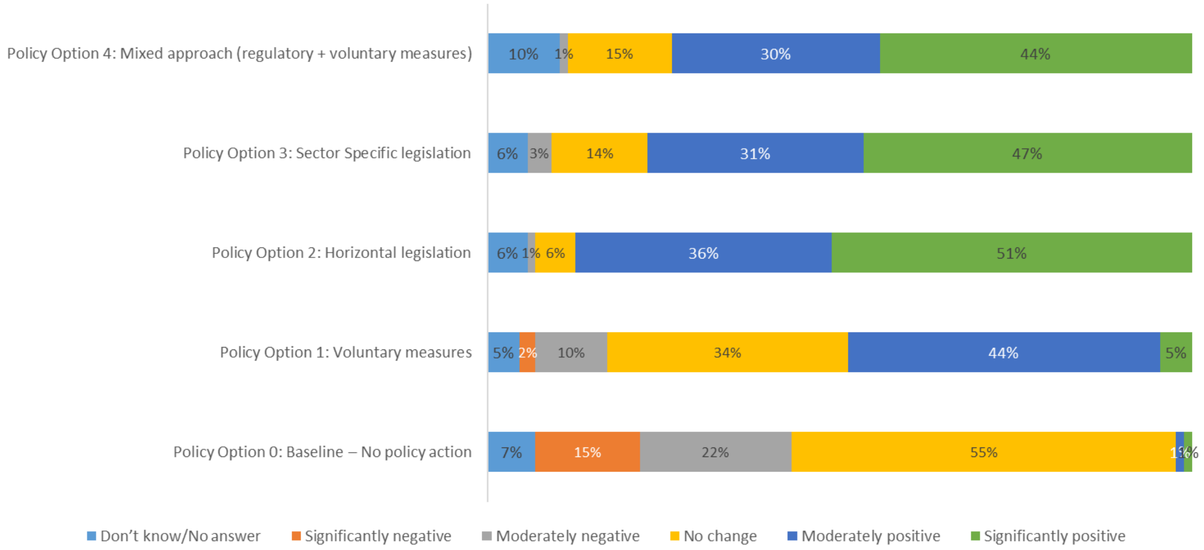


SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Once again, policy option 2 (horizontal legislation) was much more frequently deemed as having a significantly positive impact on the availability of reliable and secure ICT products in the Internal Market compared to the other policy options. Only 35% of the respondents deemed policy option 3 (sector-specific legislation) would have a significantly positive impact in this regard while 41% of the respondents thought the same about policy option 4 (mixed approach).

Like with the comments to the previous question on innovation, the most frequent comment related to the benefits of introducing horizontal legislation which would cover most ICT products with sufficiently high and uniform security standards. One NCA also added that independent conformity assessments under CSA would grant reliable and secure ICT products compare to voluntary measures.

Figure 107 Q34: What would be the impact of the policy options on the trust in ICT products?



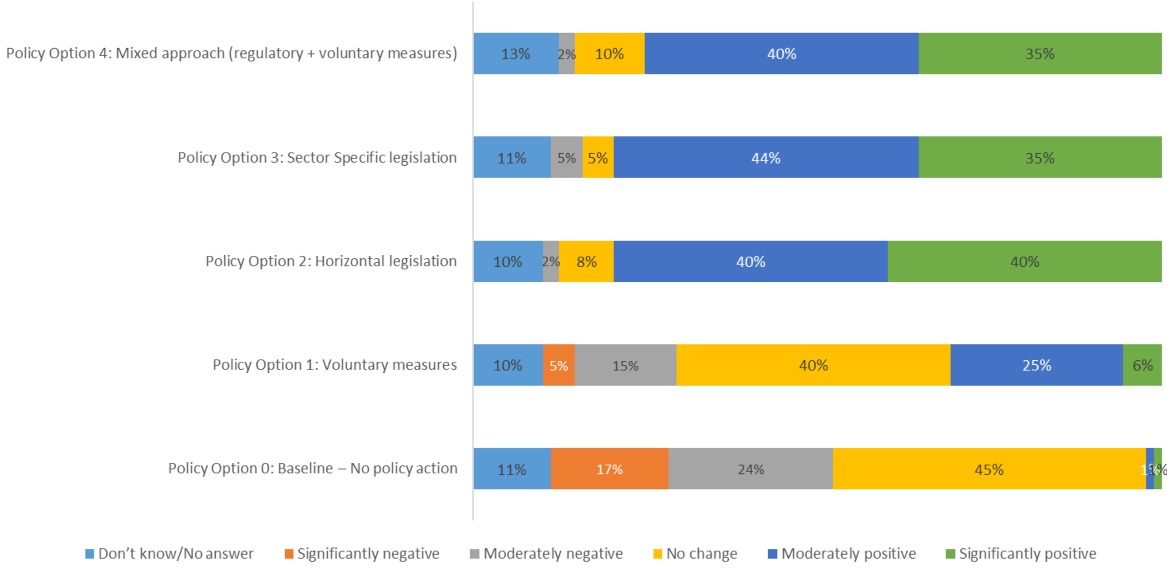
SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Policy option 2 (horizontal legislation) was deemed by the majority of the respondents (51%) to be most likely to generate a significantly positive impact regarding trust in ICT products compared to the other policy options, even if 47% and 44% of the respondents thought that policy option 3 (sector-specific legislation) and policy option 4 (mixed approach) would respectively have a significantly positive impact on trust in ICT products.

A few comments were received from the respondents in relation to the policy options' impact on trust in ICT products.

1. The most frequent comment given, especially from ICT industry players, was that sector-specific legislation would lead to fragmentation, legal uncertainty, confusing and eventually less trust in ICT products overall.
2. One respondent on behalf of the ICT industry pointed out that compliance with ICT cybersecurity laws at EU level will improve consumer trust in ICT products and that the most effective approach to achieve this would be horizontal legislation taking account of differences in risk profiles and security requirements among ICT products.
3. One respondent representing professional users remarked that improved trust will come from information to consumers; in this regard, introducing a label styled on the EU Energy Label would be desirable.

Figure 108 Q39: What would be the impact of the policy options on fundamental rights (e.g. protection of personal data, consumer protection, protection of liberty and security)?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Policy option 2 (horizontal legislation) was most frequently identified as the most effective and efficient in generating positive impact on fundamental rights, especially among respondents on behalf of the ICT industry.

A few comments were received on the policy options' potential impact on fundamental rights.

One respondent on behalf of the ICT industry commented that the most effective approach would combine a horizontal baseline of security requirements with different specific requirements for each vertical sectors.

It was remarked by three respondents that although consumer protection is a fundamental right and cybersecurity is only indirectly related, a regulation on ICT product security can be expected to impact fundamental rights positively.

One respondent on behalf of a European institution pointed out that while fundamental rights are already covered by the GDPR, the ICT industry would benefit from clear regulation and technical guidelines that would improve compliance with the GDPR.

Coherence of the policy options with other EU product safety and cybersecurity initiatives

The respondents were asked a series of questions to assess the coherence of each of the four proposed policy options with other EU initiatives in the areas of product safety and cybersecurity, such as the:

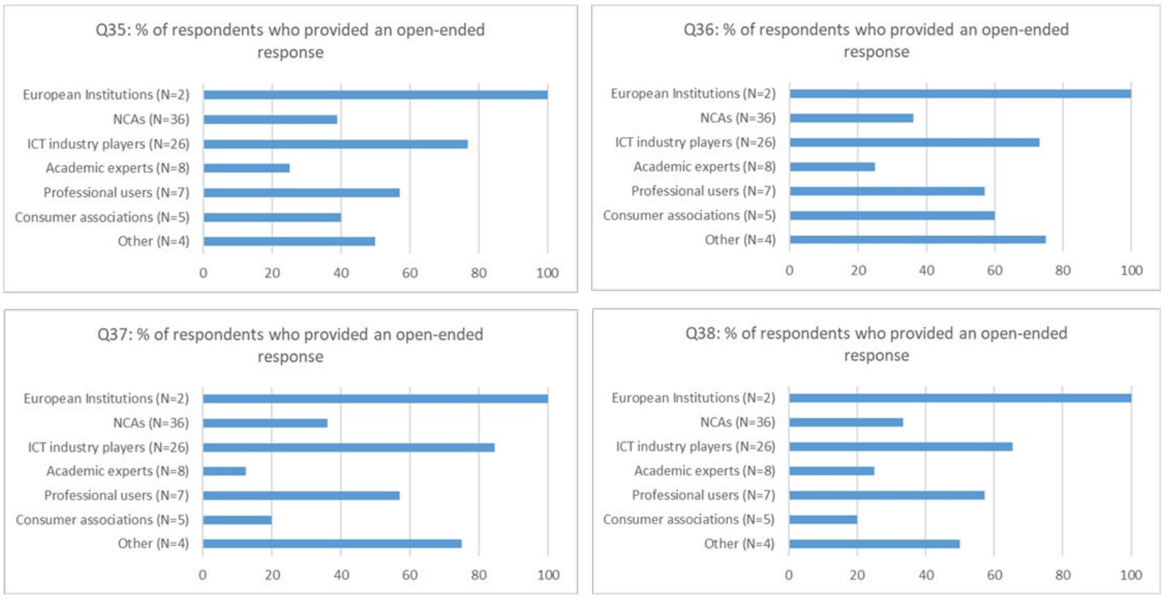
1. General Product Safety Directive,
2. Product Liability Directive,
3. Radio Equipment Directive,
4. Cybersecurity Act,
5. GDPR,

6. Machinery Directive,

7. Medical Device Regulation

These questions (Q35, Q36, Q37, Q38) were all open-ended. After cleaning for blank responses, the following charts show the percentage of respondents, by stakeholder group, who provided open-ended responses to these questions.

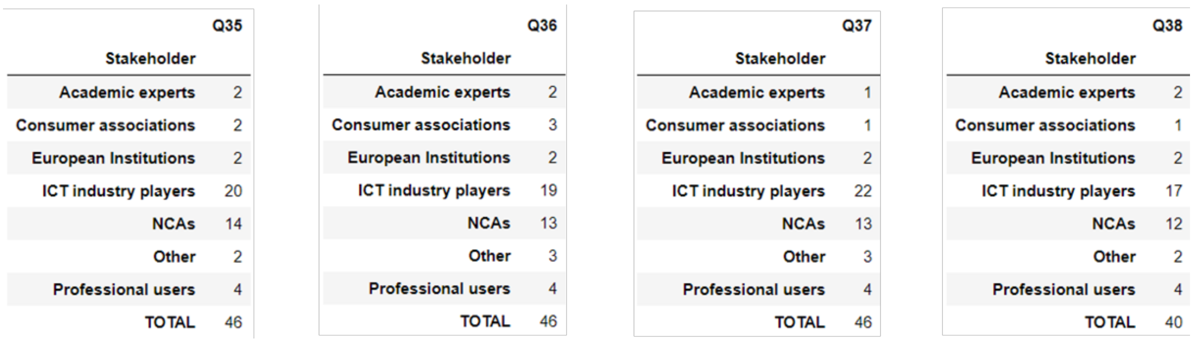
Figure 109 Percentage of respondents to the open-ended questions Q35, Q36, Q37, Q38 by stakeholder category



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

As can be seen from the below figures, around half of the total respondents (N=88) provided an open text answer to the series of questions on coherence. For all the open questions. The most represented stakeholder group is ICT industry players, followed by NCAs.

Figure 110 Number of respondents to the open-ended questions Q35, Q36, Q37, Q38 by stakeholder category



Stakeholder	Q35	Q36	Q37	Q38
Academic experts	2	2	1	2
Consumer associations	2	3	1	1
European Institutions	2	2	2	2
ICT industry players	20	19	22	17
NCAs	14	13	13	12
Other	2	3	3	2
Professional users	4	4	4	4
TOTAL	46	46	46	40

SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Question 35 asked whether **policy option 1 (voluntary measures)** would potentially not be coherent with other EU initiatives in the areas of product safety and cybersecurity such as the ones listed above.

Five respondents on behalf of NCAs expressed views that voluntary measures may lead to incoherence. Specifically, these relate to incoherence due to other initiatives such as GDPR and MDR being mandatory thereby creating a stark contrast between these and voluntary measures.

Four responding NCAs held the view that voluntary measures would not fill the gap in regulation currently existing at EU level regarding the cybersecurity of ICT products; this response may not be directly linked to coherence.

Four respondents from the ICT industry held the common view that voluntary measures could never be incoherent with legislation which companies are already compliant to.

A further ten respondents on behalf of the ICT industry believed that voluntary measures would lead to incoherence with other EU initiatives. Specific arguments include:

1. Creation of an unlevel playing field.
2. With other EU initiatives being mandated there is the potential for incoherence with voluntary measures
3. Voluntary measures may be insufficient unless driven by commercial need or regulation.
4. Potential conflicts between regulations such as CSA, NIS and NLF

Question 36 asked whether **policy option 2 (horizontal legislation)** would potentially not be coherent with other EU initiatives in the areas of product safety and cybersecurity.

Within the ICT industry players stakeholder group, the most frequent responses given were as follows:

1. Option 2 is the option that makes product policy coherent. Without such framing legislation the other regulations risk to be incoherent or even contradictive.
2. If horizontal legislation is introduced, there is no need to regulate on other initiatives. A horizontal law has the potential to yield more legal certainty and legal coherence in Europe. This would apply to all stakeholders along the value chain, which would increase the overall level of cybersecurity in the EU. The horizontal approach would make some initiatives currently under development, such as the RED delegated act, redundant since it can cover the same aspects more coherently as well as address a larger scope.

Among the other respondents on behalf of the ICT industry, eight discuss that policy option 2 would lead to incoherence with other EU initiatives. Specific concerns include:

1. The potential for overlap with other legislation.
2. Discrepancies could arise within specific sectors and/or national implementations.
3. Horizontal legislation may conflict with CSA, NIS and NLF regulation

Six respondents on behalf of NCAs shared the view that introducing horizontal legislation could lead to duplications in an effort to ensure sufficient specificity through *lex specialis* clauses. However, seven respondents on behalf of NCAs believe that whilst there could be coherence issues these could be mitigated by careful formulation or amendment of other relevant legislative acts.

Question 37 asked whether **policy option 3 (sector-specific legislation)** would potentially not be coherent with other EU initiatives in the areas of product safety and cybersecurity.

For six respondents on behalf of NCAs, policy option 3 has potential for duplication, unless existing regulation is changed so as to account for the new legislation.

Likewise, among respondents on behalf of the ICT industry, the most frequent response was that sector-specific legislation could expose industry to a set of patchy and non-aligned laws, which create inconsistent and overlapping requirements and standards.

Respondents on behalf of the ICT industry were the most vocal in terms of raising the potential issues linked to sector-specific legislation. Fifteen of them expressed concerns that Sector-specific legislation could lead to incoherence with other EU initiatives. The concerns outlined included:

1. Some products may need to implement multiple regulations.
2. Overlap and contradiction between initiatives.
3. This policy option is not necessary as existing legislation focuses on regulating Sector-specific technology.
4. Not all sectors adopt legislation thereby creating inconsistencies.

Final in the series, **Question 38** asked whether **policy option 4 (mixed approach: regulatory + voluntary measures)** would potentially not be coherent with other EU initiatives in the areas of product safety and cybersecurity.

As with policy option 3, NCAs most frequently held the view that policy option 4 would potentially lead to duplication, unless existing regulations are amended accordingly so as to account for the new legislation.

The most frequent view among respondents on behalf of the ICT industry is that the mixed approach would not add to coherence, quite the opposite.

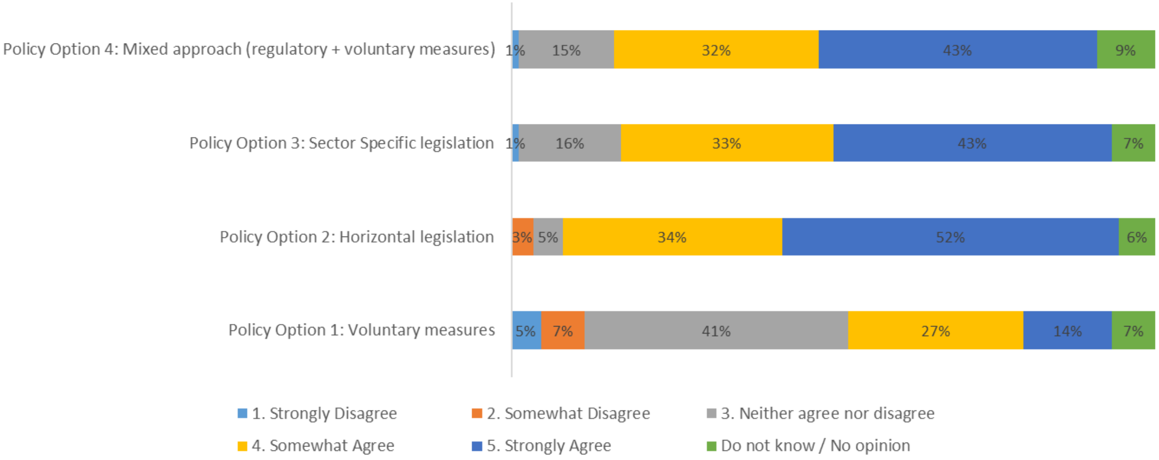
The remaining responses also generally echo the belief that a mixed approach will not necessarily lead to greater coherence with other EU initiatives with the potential for overlap/conflict between voluntary measures and legislative solutions.

In summary, of the four policy options, it appears that **respondents most frequently judged horizontal legislation to be preferable in terms of ensuring regulatory coherence** while acknowledging that voluntary measures on their own would have no effect on regulatory coherence by their very nature.

EU added value of the policy options

To conclude, the respondents were asked to indicate the extent to which they think each of the four policy options proposed would generate EU added value, if any, compared to the Member States acting alone.

Figure 111 Q40: To what extent do you agree that the policy options add EU value compared to Member States acting separately?



SOURCE: STUDY ON THE NEED OF CYBERSECURITY REQUIREMENTS FOR ICT PRODUCTS (2021), TARGETED CONSULTATION ONLINE SURVEY, N=88.

Overall, policy option 2 (horizontal legislation) was the only of the four to be deemed by the majority of the respondents (52%) as generating significant EU added value compared to Member States acting separately. Overall, 86% of the respondents agreed that horizontal legislation would generate EU added value. By comparison, only three quarters of the respondents agreed that policy options 3 and 4 would generate added value (76% and 75% respectively). Only 41% of the respondents agreed that voluntary measures would generate EU added value.

A few respondents commented on the potential EU added value of each of the four proposed policy option. Across all stakeholder groups, but particularly among respondents on behalf of the ICT industry and professional users, the most frequent comment was that the introduction of horizontal legislation (policy option 2) would generate the greatest EU added value as it would prevent market fragmentation and the emergence of Member State-specific laws on ICT product security; in other words, policy option 2 is considered as having the highest potential in contributing to the consolidation of the European Digital Single Market.

Analysis of the Position Papers

Four position papers attached to the survey responses were received through the targeted consultation. These came from:

1. BDI – Bundesverband der Deutschen Industrie e.V. (Federation of German Industries)
2. Joint position from bitkom, VDMA and ZVEI
3. Microsoft
4. VdTÜV e.V – Verband der Technischen Überwachungs-Vereine (Federation of Technical Monitoring Associations)

The key points extracted from the position papers and analysed cover the main sections of the targeted consultation questionnaire.

Problem definition – current cybersecurity issues

Three of the four position papers include general points relating to cybersecurity issues in ICT products, often with a particular focus on the responsibility of developers and manufacturers.

1. The VdTÜV e.V points out that the lack of mandatory European cybersecurity requirements is particularly critical given that cybersecurity is now recognised as playing a central role in products and companies that are increasingly dependent on digital technologies. It goes on to explain that the current lack of harmonised mandatory cybersecurity requirements and accompanying certification schemes under the CSA needs to be addressed.
2. In the context of increasing reliance on ICT, Microsoft welcomes the European Commission's effort to explore the current state of cybersecurity in broad categories of ICT products, including non-embedded software, as well as to identify the reasons for inadequate security as well as to propose relevant policies to address them. However, Microsoft adds that important opportunities would be missed by focusing solely on supply side actors and points out that all parties have a role to play in the cybersecurity of ICT products; not only stakeholders directly involved in the product throughout its entire lifecycle, but also other stakeholders such as users, security researchers, law enforcement, governments, and network providers among others.
3. The joint position from bitkom, VDMA and ZVEI points out the importance of ensuring that ICT product developers and manufacturers embed security in the design of ICT products so that they are fully compliant with Essential Requirements throughout their lifecycle; this can be done through the NLF conformity assessment procedures – i.e. internal production control in Annex II of NLF Decision No 768/2008/EC.

Cybersecurity issues as per ICT product categories and risk profiles

Points relating to the cybersecurity issues in relation to specific ICT products and their risk profiles were raised in three of the four position papers received.

1. Microsoft recommends that policy initiatives be designed to raise the cybersecurity level of all connected products to match the best practices adopted by industry leaders for security and encourages the European Commission to consider these practices and voluntary measures to ensure the proposed requirements keep pace with technology advances as well as it would allow deployers to apply the requirements proportionately to their risk profile. The paper also states a lifecycle approach to cybersecurity for ICT products – from design to maintenance – is important to capture and cover the complexity of risk profiles.
2. For the VdTÜV e.V, the CSA already offers a high degree of flexibility, whereby schemes can be developed specifically for classes of products and interacting services depending on the risk assessment by differentiating between 'basic', 'substantial' and 'high' risks. However, the position paper explains that new legislation on ICT product security is needed given that the CSA lacks the element of mandatory conformity assessment, with certification only envisaged as voluntary even for products with a high-risk profile.
3. The BDI position points out that cybersecurity measures should always be geared to products' associated risk profiles rather than having a one-size-fits-all solution. The paper explains that for instance, it would neither be technologically nor economically expedient if smart home solutions had to meet the same requirements as components that are of paramount importance for the integrity and availability of critical infrastructures.

4. Policy options for ICT cybersecurity

5. Potential future regulatory developments were a central part of the four position papers received through this targeted consultation. The points frequently made are that any new regulatory action should avoid any overlaps with the CSA and duplication of efforts and that horizontal regulation on ICT product security with basic mandatory requirements and standards would be the best way forward:

6. Microsoft recommends avoiding a future patchwork of complex legislation when the EU already has significant cybersecurity activities; examples given are the development and adoption of certification schemes for the CSA, standards development to support the RED delegated acts, and the NIS 2.0 Directive. Microsoft therefore recommends aligning the Commission's legislative objectives with existing cybersecurity policy or legislation and any new regulatory policy options with other international baselines or harmonised efforts. For Microsoft, duplication of both existing requirements and voluntary provisions under the existing legislative frameworks should be avoided.

7. The VdTÜV e.V points out that the CSA holistically covers cybersecurity risks by not only applying to products but also services and processes. The added value of the CSA compared to sector-specific directives and regulations for product safety thus primarily lies in the horizontal approach, which can identify cyber risks across all sectors which facilitates the specification of requirements for both uniform cybersecurity measures and assessment procedures without differentiating between products and IT services – a differentiation which is difficult in practice. The position paper goes on to recommend the option of introducing a lean singular horizontal regulation setting out basic mandatory cybersecurity requirements that apply to all products covered by the NLF, irrespective of the sector, but otherwise referring to the CSA mandatory schemes when it comes to conformity assessment procedures. This would effectively make CSA schemes mandatory for all ICT products (depending on the existence of such a scheme for a specific products). In other words, a horizontal cybersecurity regulation would refer to the CSA schemes instead of harmonised standards insofar as such schemes have been developed for specific products or services. This approach would also make the CSA schemes mandatory for sector-specific directives and regulations. The corresponding conformity assessment procedures or risk levels (i.e. basic, substantial, high) should then also be adopted. For the VdTÜV e.V, only such a procedure would avoid unnecessary duplication and potential inconsistencies between product safety legislation and the CSA.

8. For the BDI, binding protection targets should be defined by law and specified by harmonised European standards that reflect the dynamic development of the state of the art so as to achieve overarching cyber resilience. The Digital Single Market will only be successful if national isolated solutions are avoided and compatibility with international standards is ensured.

9. The joint position from bitkom, VDMA and ZVEI calls for a horizontal regulation adhering to the NLF under which security support is already part of manufacturers' obligations. In a context where cybersecurity is a dynamic process, security support is required in the form of ICT product updates. The position papers specifies that ICT security support should be embedded in the chapter on manufacturer obligations which is foreseen in the reference provisions of the NLF.

Impacts of the proposed policy options

Points were made relating to the potential impacts of different possible options for future legislation on the security of ICT products. There were also points relating to the potential added value of current and future EU legislation in the area of ICT products.

1. For Microsoft, any new legislation, even if written as requirements for a limited set of stakeholders, could have unexpected impacts on other stakeholders. It is imperative that the development of new policy tools is transparent, open, engages diverse stakeholders, and provides sufficient clarity of scope, and trumps policy development with adequate time periods for critical analysis and feedback.
2. For the BDI, all stakeholders must contribute their share to ensure a risk-adequate level of cybersecurity, manufacturers and private and commercial users alike. Since products intended for commercial and private use are connected, it would be insufficient if only some users and manufacturers were investing in cybersecurity. Consequently, success for the BDI lies in a holistic strengthening of the cybersecurity level across Europe, which can only be achieved if all act in concert and the measures are coordinated. Holistic cybersecurity strategies with efficient protective measures will have the greatest positive impact on cyber resilience. The goal must be to close dangerous gaps and vulnerabilities by taking swift and appropriate action to prevent potential attackers from exploiting them.
3. For VdTÜV e.V, the added value of the CSA lies in the horizontal, uniform regulation of cybersecurity requirements, the inclusion of ICT products as well as of ICT services and processes, uniform requirements for assessment and certification procedures, and a risk-based approach.

Conclusions of the targeted consultation

Regarding the **problem definition**, to gauge the need for new legislation on ICT cybersecurity, 43% of the respondents to the targeted consultation thought the level of security of ICT products available in the EU was fair. There was an equal proportion of respondents who thought that the level of security of ICT products is either poor or good (24%). Only 7% of the respondents thought this level to be very high or excellent.

There was general agreement that there was still a lack of security around ICT products, with the causes most frequently cited by the respondent for this being the lack of qualified security professionals, no harmonised conformity assessment across the EU, no rules for post-market surveillance, no mandatory obligations for manufacturers, and no common legal basis that sets cybersecurity requirements for ICT products.

According to the respondents, the main reason for insufficient understanding of ICT cybersecurity among professional users and private users (or citizens at large) was information asymmetry in relation to the cybersecurity properties of ICT products.

Regarding **sector-specific cyberthreats and risk profiles**, the energy was most frequently deemed by the respondent as facing the highest threats, followed by transport, smart manufacturing and smart home. Over three-quarters of the respondents thought that Essential Requirements (ER) to ensure cybersecurity should target ICT products before and after market placement while 22% indicated they should only apply before market placement.

Regarding the **proposed policy options**, most of the respondents (56%) rated voluntary measures as addressing the need for cybersecurity for ICT products to a small or very small extent.

Conversely, the same proportion of respondents (56%) rated the introduction of horizontal legislation as addressing the need for cybersecurity for ICT products to a large or very large extent. Similarly, 55% of the respondents rated the introduction of new sector-specific legislation as addressing the need for cybersecurity for ICT products to a large or very large extent – however, respondents frequently pointed out that sector-specific legislation should serve to complement horizontal legislation.

Regarding the mixed approach option (regulatory + voluntary measures), fewer respondents found this to be relevant to the need to ensure cybersecurity in ICT products; a reason frequently given by the respondents was that this option would cause regulatory complexity, market fragmentation and confusion.

Regarding the **potential impacts** of the four policy options proposed, horizontal legislation was most frequently judged by the respondents to be the most cost-effective and the most likely to contribute to the consolidation of the European Digital Single Market.

Overall, respondents to the targeted consultation frequently held the view that any regulatory action should avoid any overlaps with the CSA and duplication of efforts and that horizontal legislation with mandatory requirements applying to all ICT products covered under the NLF would generate the greatest EU added value.