POSITION PAPER

ESBG response to the EC public consultation on the Cyber Resilience Act

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

May 2022

ESBG

Introduction

Digital products and ancillary services create significant opportunities for EU economies and societies, along with new challenges that need to be addressed. In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply-chain. It can lead to severe disruption of economic and social activities or even become life threatening. The lack of appropriate security in digital products and services constitutes one of the main avenues for successful attacks.

In her State of the Union 2021 address, President von der Leyen underlined that the EU should not merely settle to address the cyber threats, but also strive to become a leader in cybersecurity. This could be achieved through legislation on horizontal requirements under a new European Cyber Resilience Act, included in the Commission Work Programme for 2022 under the headline ambition "A Europe Fit for the Digital Age". This comes against the background of a growing number of high-profile cyberattacks with a global footprint: the annual cost of cybercrime to the global economy in 2020 was estimated to be EUR 5.5 trillion, double that of 2015 (JRC, Cybersecurity – Our Digital Anchor, 2020). It is also partly a result of suboptimal cybersecurity measures for digital products and ancillary services. The new European Cyber Resilience Act will also contribute to the EU's continuous effort for an effective and genuine Security Union in the digital era.

This public consultation aims at informing the Commission's upcoming Cyber Resilience Act initiative. Your answers will help the Commission analyse cybersecurity-related problems associated with the digital products markets, explore possible ways forward and assess the impact of different types of interventions.

Please note that the translations of this consultation in the other EU languages will follow.

This consultation will remain open until 25 May 2022.

Definitions

For the purposes of this public consultation, the notion of **digital product** covers both hardware and software products. A **hardware product** is defined as any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data. A **software product** is defined as an intangible good that processes digital data, stored, retrieved or transmitted by a hardware device, by executing encoded instructions. Software products include for example operating systems, user applications or firmware. Software can be made available without hardware (so-called '**non-embedded software**' or standalone software) or as specialised software directly supportive to the function of the hardware product on which the software is run (so-called '**embedded software**'). **Ancillary service** means a (digital) service, the absence of which would prevent the tangible product from performing its functions (e.g. a website through which you access to the functionality of a device). **Cybersecurity** means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats (Article 2(1) of EU Cybersecurity Act).

How to respond to the questionnaire

The questionnaire and all its questions are open to everyone, from ordinary consumers to cybersecurity experts and other potentially affected stakeholders. In addition, to facilitate responding to the questionnaire, the questions have been grouped into different categories requiring different types of expertise:

- **Section 1** contains questions on the state of cybersecurity of digital products and users' ability to choose secure products and use them in a secure manner.
- **Section 2** explores various options to improve the cybersecurity of digital products. This includes also questions on the types of products to be covered by an intervention, on other relevant legislation, on security requirements, on the notion of risk, as well as ways to assess the conformity of vendors.
- **Section 3** focuses on the EU added value and the estimated impacts of potential measures on stakeholders.
- **Section 4** focuses on cybersecurity challenges for the internal market other than those related to digital products.

Whenever the questionnaire refers to 'users', the term encompasses both consumers using digital products as well as businesses, public authorities and other types of organisations deploying digital products. Whenever the questionnaire refers to 'vendors', the term encompasses hardware manufacturers, software developers as well as distributors (e.g. retailers) and importers of digital products.

Please note that you can also upload a document (e.g. position paper) at the end of the questionnaire.

Section 1: Cybersecurity of digital products and the users of digital products

This section contains questions on the state of cybersecurity of digital products marketed in the European Union and users' ability to choose secure products and use them in a secure manner, and the role that vendors can play in securing products and providing cybersecurity related information on their products.

Sub-section 1.a. – The state of cybersecurity of digital products

Q1: In your view, what is the overall level of cybersecurity of digital products marketed within the European Union (on a scale from 1 to 5 with 5 indicating a very high level of cybersecurity)?

1	2	3	4	5	Don't know/no opinion
		X			

Please elaborate *(1000 characters max)*

Q2: In your view, during the last five years, how has the level of risk of cybersecurity incidents affecting digital products evolved?

	Risk level has decreased significantly
	Risk level has decreased
	Risk level is the same
x	Risk level has increased
	Risk level has increased significantly
	I don't know/no opinion

Please elaborate *(1000 characters max)*

Sub-section 1.b. – Consequences of cyber incidents and non-secure digital products

Q3: **How would you evaluate the actual impact of cybersecurity incidents affecting digital products on you or your organisation (on a scale from 1 to 5 with 5 indicating a very high negative impact)?**

	1	2	3	4	5	I don't know / no opinion
Financial cost of implementing measures to respond to a cybersecurity incident				x		
Financial cost of disruption (e.g. due to a ransomware attack)				x		
Reputational damage				x		
Compromising the security of our economy and society				x		
Damage to health and life		x				
Damage to fundamental rights (e.g. privacy, protection of personal data, consumer protection)				x		

Environmental damage		x				

Please elaborate, if possible quantify *(1000 characters max)*

Q4: In your view, if a digital product is not cyber secure, how does it impact the user (on a scale from 1 to 5 with 5 indicating that you fully agree)?

	1	**2**	**3**	**4**	**5**	**I don't know / no opinion**
The user bears additional cost when affected by a cybersecurity incident					x	
The user bears additional costs due to highly priced cybersecurity insurance					x	
The user bears additional costs due to the need to deploy highly priced technical security solutions					x	

Please elaborate, if possible quantify *(1000 characters max)*

Sub-section 1.c. – Trust, cybersecurity awareness and capabilities of users

Q5: To what extent do you agree with the following statements as regards your awareness and understanding of cybersecurity properties of digital products (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

	1	**2**	**3**	**4**	**5**	**I don't know / no opinion**
In general terms, I am aware of the cybersecurity risks associated with digital products					x	

There is sufficient and clear information made available on the cybersecurity properties of digital products		x				
I understand the cybersecurity properties I should expect from a product and have the skills to operate it securely					x	
I value aspects of usability and price of a digital product higher than its cybersecurity features			x			

Sub-section 1.d - The role of vendors in providing secure digital products

Q6: To what extent do you agree with the following statements on the role of the vendors? Please rate the following statements on a scale from 1 to 5 (with 5 indicating that you strongly agree).

	1	2	3	4	5	I don't know / no opinion
Vendors of hardware are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers			x			
Vendors of software are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers			x			

Q7: <u>If you are a vendor:</u> which of the following aspects have the biggest impact on your decision related to cybersecurity of your digital product?

	Very relevant	Relevant	Neither nor	Not too relevant	Not relevant at all	Don't know / no opinion
The potential reputational damage and the loss of trust of the users following an incident	x					
Customer expectations, including contractual obligations	x					
Public procurement practices (e.g. guidelines)		x				

What are other aspects affecting your decision related to cybersecurity of your digital product? *(1000 characters max)*

Good practices / regulatory compliance

Q8: To what extent are hardware manufacturers and software developers taking the cybersecurity of their digital products into account in each of the following phases of the product lifecycle (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously)?

	1	2	3	4	5	I don't know / no opinion
Design			x			
Development			x			
Delivery of the product on the market			x			
Maintenance and evolution of the product (e.g. after-sale)				x		

Section 2: Improving the cybersecurity of digital products

This section explores various policy options to improve the cybersecurity of digital products. This includes also questions on the types of products to be covered by an intervention, on other relevant legislation, on security requirements, on risk as well as ways to assess the conformity of manufacturers.

Sub-section 2.a. – Exploring ways to make digital products more secure

Q9: To what extent do you think that the following measures could be effective in raising the level of cybersecurity of digital products marketed in the Union (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

	1	2	3	4	5	I don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors				x		

Further voluntary European cybersecurity certification schemes for digital products and services			x			
EU public procurement guidelines taking into account cybersecurity requirements			x			
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)			x			
Introducing mandatory horizontal cybersecurity requirements for hardware products				x		
Introducing mandatory horizontal cybersecurity requirements for software products				x		

Please elaborate *(1000 characters max)*

Q10: How would you assess the impact of the following measures on the level of cyber-security of digital products and of the consumers/organisations using such products (on a scale from 1 to 5 with 5 indicating that a measure would have a very high impact)?

	1	**2**	**3**	**4**	**5**	**I don't know / no opinion**
Require vendors to make available information and provide instructions on securely installing, operating and using the product in question				x		
Require vendors to take corrective actions (such as patching, recalling or withdrawing a product) when a product is found to be not secure					x	

Sub-section 2.b. – Exploring ways to make users more aware

Q11: How would you assess the relevance of the following measures for the users' ability to evaluate the cybersecurity properties of a digital product and to make better informed purchase or usage decisions (on a scale from 1 to 5 with 5 indicating that a measure is very relevant)?

	1	2	3	4	5	I don't know / no opinion
Making available technical documentation (containing information to demonstrate the conformity of the product to the applicable requirements) on the cybersecurity properties of a product (such as on risks and proper use)			x			
Making available EU Declaration of conformity (stating that all the relevant requirements of the applicable legislation are satisfied)				x		
Affixed symbol of compliance (such as CE marking)				x		
Training on the secure use of digital products				x		

Which other measures would allow for better informed purchase or usage decisions by the user? Please elaborate *(1000 characters max)*

Sub-section 2.c. – Digital products to be covered by a European initiative

Q12: To what extent do you agree that subjecting certain products marketed in the Union to cybersecurity requirements would be effective (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

	1	2	3	4	5	I don't know / no opinion
Hardware products				x		
Embedded software				x		
Ancillary services				x		
Hardware products subject to higher cybersecurity risks					x	

All standalone software products				x		
Software products subject to higher cybersecurity risk					x	

Please elaborate *(1000 characters max)*

Sub-section 2.d. – Existing legislation on the cybersecurity of digital products

Q13: To what extent do you agree with the following statements about how cybersecurity is addressed in existing EU legislation (e.g. the General Product Safety Directive and the Machinery Directive, both currently under review; the Delegated Regulation of 29 October 2021 under the Radio Equipment Directive) (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	I don't know / no opinion
Existing EU regulation appropriately addresses cybersecurity of tangible digital products (hardware) throughout their lifecycle						x
Existing EU regulation appropriately addresses cybersecurity of intangible digital products (software) throughout their lifecycle						x
Existing EU regulation appropriately addresses all relevant cybersecurity risks (material and non-material damages) related to the use or misuse of a digital product						x

Q14: In the absence of horizontal cybersecurity requirements at European level, Member States could adopt national laws placing certain requirements on vendors. To what extent do you agree that there is a risk of increasing costs and legal uncertainty for market stakeholders, in the absence of an EU initiative? (on a scale from 1 to 5 with 5 indicating you fully agree)?

	1
	2
	3
	4
x	5
	I don't know / No opinion

Please elaborate *(1000 characters max)*

Q15: If you are a vendor: are your digital products subject to legal requirements as regards their cybersecurity? In your answer, please take into account European, national but also legislation stemming from third countries.

	Yes
	No
x	I am not concerned by this question
	I don't know / No opinion

Sub-section 2.e. – Cybersecurity requirements for digital products

Q16: Should hardware manufacturers and software developers be responsible for the full life cycle of a digital product (such as by being required to provide updates)?

x	Yes
	No
	I do not know / No opinion

Please elaborate *(1000 characters max)*

Q17: To what extent can the following approaches contribute to the cybersecurity of a digital product (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

	1	2	3	4	5	I don't know / no opinion
Cybersecurity is taken into account during all phases of the development process (security by design)					x	
Products are placed on the market with the most secure settings enabled by default (security by default)				x		
Hardware manufacturers and software developers should make available to relevant stakeholders (e.g. end-users) a list containing the details and supply chain relationships of			x			

various components used in building the digital product (so-called (Software) Bill of Materials)						
Products should be designed in such a way that they are fully updatable					x	
Hardware manufacturers and software developers provide updates when vulnerabilities are discovered, including after a product has been put on the market					x	
Hardware manufacturers and software developers should provide updates free of charge					x	
Hardware manufacturers and software developers facilitate vulnerability disclosure (e.g. by public authorities; independent researchers)				x		
Products must feature all the necessary functional (e.g. two-factor authentication) and non-functional (e.g. resilience against DDoS (Distributed Denial of Services) attacks) security requirements				x		

Which other measures taken by hardware manufacturers and software developers could improve the cybersecurity of digital products? *(1000 characters max)*

Sub-section 2.f. – The role of risk

Q18: Under this initiative, hardware manufacturers and software developers would need to demonstrate their compliance with cybersecurity requirements. Should digital products with a higher risk be subject to a stricter process of demonstrating conformity with these requirements?

x	Yes
	No
	I do not know / No opinion

Sub-section 2.g. – Demonstrating compliance with security requirements

Q19: How would you assess the following statement regarding self-declaration as a way for hardware manufacturers and software developers to demonstrate compliance with security requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

	1	2	3	4	5	I don't know / no opinion
A self-declaration of conformity by a hardware manufacturer or software developer gives a sufficient confidence that security requirements are met		x				

Q20: If you consider that self-declaration is not enough to demonstrate compliance with security requirements, do you think that the involvement of a third party should be required under certain circumstances?

x	Yes
	No
	I do not know / No opinion

Please elaborate *(1000 characters max)*

We consider that the self-declaration is not enough to demonstrate compliance with the security requirements, and that it would be more valuable to have the opinion of a third party based on a control framework.

Section 3: Stakeholder impact of potential regulatory measures

This section focuses on the EU added value and estimated impacts of potential measures on stakeholders.

Sub-section 3.a. – Relevance of horizontal requirements for digital products at European level

Q21: To what extent do you agree with the following statements that look into the potential effectiveness of an EU initiative on horizontal (cross-sectoral) cybersecurity requirements?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Cyber risks can propagate across borders and sectors at high speed, which is why cybersecurity rules for digital products should be aligned at Union level				x	
Horizontal cybersecurity requirements for digital products would increase awareness of users when it comes to cyber risks			x		
Horizontal cybersecurity requirements for digital products would enhance and ensure a consistently high level of the security of digital products and ancillary services			x		
Horizontal cybersecurity requirement would improve the functioning of the internal market by levelling the playing field for vendors of digital products and ancillary services as regards cybersecurity features		x			

Q22: The EU Action Plan on synergies between civil, defence and space industries underlines the importance of promoting and applying common standards across sectors and the increased relevance of digital products that are used both in a civilian and military context ('dual-use products'). To what extent could horizontal requirements applying to digital dual-use products contribute to moving the security performance of such products closer to the needs of the defense community and to raising the overall level of cybersecurity in civilian uses (on a scale from 1 to 5 with 5 indicating a very positive contribution)?

1	2	3	4	5	I don't know / no opinion
					x

Please elaborate *(1000 characters max)*

Sub-section 3.b. – Impact on your organisation in terms of cost

Q23: How would you assess the impact of the following types of intervention on the costs of your organisation (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly)?

	1	2	3	4	5	I don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors					x	
Further voluntary European cybersecurity certification schemes for digital products and services				x		
EU public procurement guidelines taking into account cybersecurity requirements				x		
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)	x					
Introducing mandatory horizontal cybersecurity requirements for hardware products				x		
Introducing mandatory horizontal cybersecurity requirements for software products				x		

Please elaborate your answer, by quantifying the costs if possible *(1000 characters max)*

We don't have data to answer this question.

Sub-section 3.c. – Regulatory burden and costs for small and medium-sized companies

Q24: Which of the following approaches would in your view ensure that small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs, are subject to proportionate obligations (balance between administrative burden and compliance costs on the one hand and a high level of cybersecurity on the other hand) under a European legislation introducing mandatory horizontal cybersecurity requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	I don't know / no opinion
Subject small and medium-sized companies to the same obligations as larger companies			x			
Introduce simplified procedures to demonstrate conformity for small companies and individual entrepreneurs			x			

Which other approaches could ensure proportionate obligations vis-à-vis small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs? *(1000 characters max)*

Sub-section 3.d. – Impact on competition

Q25: An EU initiative laying down mandatory horizontal cybersecurity requirements would apply to all vendors placing products on the internal market, irrespective of their origin and location. To what extent would you agree with the following statements regarding the impact on competition of such an initiative (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	I don't know / no opinion
Mandatory cybersecurity requirements will put smaller hardware manufacturers and software developers at a disadvantage compared with larger competitors				x		
Mandatory cybersecurity requirements will put EU manufacturers and software developers at a disadvantage on the non-EU markets compared to non-EU					x	

competitors that are not subject to such requirements						

Sub-section 3.e. – Impact on fundamental rights

Q26: To what extent to you agree with the following statements regarding the impact of horizontal cybersecurity requirements on fundamental rights (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	I don't know / no opinion
Horizontal cybersecurity requirements for digital products would enhance protection of privacy and personal data			x			
Horizontal cybersecurity requirements for digital products would ensure a high level of consumer protection				x		

Section 4: Other issues

This section focuses on cybersecurity challenges for the internal market other than those related to digital products.

Q27: In addition to the issues above, are there other cybersecurity related challenges not directly linked to the cybersecurity of products that you think the Cyber Resilience Act should include to enhance the cyber resilience of the internal market? Please elaborate

(1000 characters max)

About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 17 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion billion in corporate loans, including SMEs, and serve 163 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. May 2022.