Contribution ID: 224b2836-4291-4356-bb0b-2820fc175a34
Date: 25/05/2022 16:00:54

Public Consultation on the cybersecurity of digital products and ancillary services

Fields marked with * are mandatory.

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).

About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- (•) English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Irish
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- Academic/research institution
- Business association

- ○ Company/business organisation
- ○ Consumer organisation
- ○ EU citizen
- ○ Environmental organisation
- ○ Non-EU citizen
- ○ Non-governmental organisation (NGO)
- ○ Public authority
- ◉ Trade union
- ○ Other

* First name

Simon

* Surname

Jernberg

* Email (this won't be published)

sje@nordicfinancialunions.org

* Organisation name

255 character(s) maximum

Nordic Financial Unions

* Organisation size

- ◉ Micro (1 to 9 employees)
- ○ Small (10 to 49 employees)
- ○ Medium (50 to 249 employees)
- ○ Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

4129929362-47

*

Country of origin

Please add your country of origin, or that of your organisation.

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname

- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Myanmar/Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom

- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

Please specify in which capacity are you responding to this questionnaire.

- User of digital product
- Software developer
- Hardware manufacturer
- Notified body
- Accreditation body
- Market Surveillance Authority
- Importer of hard- or software
- Distributor (e.g. Retailer)
- Other

If you have selected 'Other', please state in which capacity are you replying to this questionnaire.

Trade union in the finance sector

Before starting this survey, please indicate if you have expert knowledge in cybersecurity regulation?

- ○ *Yes*
- ◉ *No*

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association, 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* **Contribution publication privacy settings**

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- ◉ **Anonymous**
  Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.
- ○ **Public**
  Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

☑ I agree with the personal data protection provisions

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

Please elaborate

1000 character(s) maximum

Overall, we see that the cybersecurity in the finance sector is ok. However, with the rapid digitalisation of the sector, and interconnectedness we can also see that the cyber risks and threats are increasing. Financial actors and regulators should address this. NFU welcomes that the Commission is addressing cybersecurity and the vulnerability that digital products or services can have when not fully controlled.

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
- ○ Risk level has increased
- ◉ Risk level has increased significantly
- ○ Don't know / no opinion

Please elaborate

1000 character(s) maximum

We can clearly see that threats to cybersecurity of financial companies have increased parallel to the digital development of the sector. The Nordic financial sector is especially digital and dependent on digital products and infrastructure to function. This development have also lead to that many financial actors become dependent on purchasing digital services from tech suppliers. This development has raised the risks and we see a clear need for strengthened cyber resilience.
The financial sector is built on and dependent on trust from customers and society. Therefore, it is of utmost importance that the society can trust that essential services, such as payments, savings, insurance, and access to bank accounts, can function at all times. Financial companies deal with a lot of data and often sensitive data on customers and companies, and risks to cybersecurity in financial services is including big risks to these data.

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	Don't know / no opinion
Financial cost of implementing measures to respond to a cybersecurity incident	○	○	○	○	◉	○
Financial cost of disruption (e.g. due to a ransomware attack)	○	◉	○	○	○	○
Reputational damage	○	○	○	○	◉	○
Compromising the security of our economy and society	○	○	○	○	◉	○
Damage to health and life	○	◉	○	○	○	○

Damage to fundamental rights (e.g. privacy, protection of personal data, consumer protection)	○	○	○	○	◉	○
Environmental damage	○	◉	○	○	○	○

Please elaborate, if possible quantify

1000 character(s) maximum

Nordic finance companies invest a lot in digital and cybersecurity.
Financial employees are at the very heart of this development, being the ones that need to implement digital tools and dealing with sensitive financial information and data. They also deal with a lot of private data of customers and companies.
NFU sees an enormous need for training, competence development and resources for financial employees to be able to measure up with the digital development in finance and to be able to keep up with and address cybersecurity risks. We can't stress enough the need for competence and learning on issues such as cybersecurity, data privacy and compliance. NFU and its member unions see a development where many financial employees struggle with keeping up with the digital development, something that can become a cyber risk. Companies have an important role to provide this training and accurate resources for financial employees.

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	Don't know / no opinion
The user bears additional cost when affected by a cybersecurity incident	○	○	○	○	○	◉
The user bears additional costs due to highly priced cybersecurity insurance	○	○	○	○	○	◉
The user bears additional costs due to the need to deploy highly priced technical security solutions	○	○	○	○	○	◉

Please elaborate, if possible quantify

1000 character(s) maximum

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	Don't know / no opinion
In general terms, I am aware of the cybersecurity risks associated with digital products	○	○	○	○	○	◉
There is sufficient and clear information made available on the cybersecurity properties of digital products	○	○	○	○	○	◉
I understand the cybersecurity properties I should expect from a product and have the skills to operate it securely	○	○	○	○	○	◉
I value aspects of usability and price of a digital product higher than its cybersecurity features	○	○	○	○	○	◉

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	Don't know / no opinion
Vendors of hardware are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers	○	○	○	○	○	◉
Vendors of software are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers	○	○	○	○	○	◉

Q7: If you are a vendor: 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	○	○	○	○	○	◉
Customer expectations, including contractual obligations	○	○	○	○	○	◉

Public procurement practices (e. g. guidelines)	○	○	○	○	○	◉

What are other aspects affecting your decision related to cybersecurity of your digital product?

1000 character(s) maximum

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	Don't know / no opinion
Design	○	○	○	○	○	◉
Development	○	○	○	○	○	◉
Delivery of the product on the market	○	○	○	○	○	◉
Maintenance and evolution of the product (e.g. after-sale)	○	○	○	○	○	◉

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	Don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors	○	○	○	○	◉	○

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

Please elaborate

1000 character(s) maximum

NFU welcomes that the Commission is addressing cybersecurity and the vulnerability that digital products or services can have when not fully controlled.
On the other hand, regulation and demand on complex digital regulation must be done in a way that is proportional. Financial employees are already subject to a massive amount of regulatory frameworks in their job. It is therefore important that an employee perspective is applied when setting up regulation, bearing in mind that financial employees are the ones that will apply the rules in practice. This will also require education and training for employees.
A good starting point when discussing potential regulation on digital products is to go by the rule “same risk – same regulation”.

Q10: How would you assess the impact of the following measures on the level of cybersecurity 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	Don't know / no opinion
Require vendors to make available information and provide instructions on securely installing, operating and using the product in question	○	○	○	○	◉	○
Require vendors to take corrective actions (such as patching, recalling or withdrawing a product) when a product is found to be not secure	○	○	○	○	◉	○

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	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)	○	○	○	◉	○	○
Making available EU Declaration of conformity (stating that all the relevant requirements of the applicable legislation are satisfied)	○	○	◉	○	○	○
Affixed symbol of compliance (such as CE marking)	○	○	◉	○	○	○
Training on the secure use of digital products	○	○	○	○	◉	○

Which other measures would allow for better informed purchase or usage decisions by the user? Please elaborate

1000 character(s) maximum

NFU sees an enormous need for training, competence development and resources for financial employees to be able to measure up with the digital development in finance and to be able to keep up with and address cybersecurity risks. We can't stress enough the need for competence and learning on issues such as cybersecurity, data privacy and compliance. NFU and its member unions see a development where many financial employees struggle with keeping up with the digital development, something that can become a cyber risk. Companies have an important role to provide this training and accurate resources for financial employees.

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	Don't know / no opinion
Hardware products	○	○	○	○	○	◉
Embedded software	○	○	○	○	○	◉
Ancillary services	○	○	○	○	○	◉

Hardware products subject to higher cybersecurity risks	○	○	○	○	○	◉
All standalone software products	○	○	○	○	○	◉
Software products subject to higher cybersecurity risk	○	○	○	○	○	◉

Please elaborate

1000 character(s) maximum

The Nordic financial sector is especially digital and dependent on digital products and infrastructure to function. This development have also lead to that many financial actors become dependent on purchasing digital services from tech suppliers. This development has raised the risks and we see a clear need for strengthened cyber resilience.

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	Don't know / no opinion
Existing EU regulation appropriately addresses cybersecurity of tangible digital products (hardware) throughout their lifecycle	○	○	◉	○	○	○
Existing EU regulation appropriately addresses cybersecurity of intangible digital products (software) throughout their lifecycle	○	○	◉	○	○	○
Existing EU regulation appropriately addresses all relevant cybersecurity risks (material and non-material damages) related to the use or misuse of a digital product	○	○	◉	○	○	○

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
- 5
- Don't know / no opinion

Please elaborate

1000 character(s) maximum

The digital development in finance is rapid, and with it the interconnectedness is increased. When a sector is going digital it is also going global/international. To be able to control and manage the risks conncted to this development, there are arguments for that there is a need to address this at global/EU level.

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
- I am not concerned by this question
- 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)?

- Yes
- No
- Don't know / no opinion

Q16a: If you think that hardware manufacturers and software developers should be required to provide security updates, for how many years should they be required to do so?

- 1
- 2
- 3
- 4
- 5
- 6

- 7
- 8
- 9
- 10
- Don't know / no opinion
- Other (please specify below)

Please elaborate

1000 character(s) maximum

This is something that must be extremely clear. The financial sector is built on and dependent on trust from customers and society. Therefore, it is of utmost importance that the society can trust that essential services, such as payments, savings, insurance, and access to bank accounts, can function at all times. The cyber resilience of financial services is key here. Many financial actors become dependent on purchasing digital services from tech suppliers. In cloud services, it must be clear that the supplier is responsible. When a service/product is bought, it must also be clear who is baring the risk responsibility.
It must be extremely obvious in regulation and legislation who bares the responsibility.

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	Don't know / no opinion
Cybersecurity is taken into account during all phases of the development process (security by design)	○	○	○	○	○	◉
Products are placed on the market with the most secure settings enabled by default (security by default)	○	○	○	○	○	◉
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 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	○	○	○	○	○	◉
Hardware manufacturers and software developers provide updates when vulnerabilities are discovered, including after a product has been put on the market	○	○	○	○	○	◉
Hardware manufacturers and software developers should provide updates free of charge	○	○	○	○	○	◉

Hardware manufacturers and software developers facilitate vulnerability disclosure (e.g. by public authorities; independent researchers)	○	○	○	○	○	◉
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	○	○	○	○	○	◉

Which other measures taken by hardware manufacturers and software developers could improve the cybersecurity of digital products?

1000 character(s) maximum

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?

- ◉ Yes
- ○ No
- ○ Don't know / no opinion

Q18a: The way hardware manufacturers and software developers would be required to demonstrate their compliance with cybersecurity requirements could be made dependent on the risk associated with a specific product. What categories of risk should such a risk-based methodology take into account? *(multiple answers are possible)*

- ☐ The functionality of a product (such as whether it has a network interface or not, or whether it controls certain security features of a digital system)
- ☐ The societal importance of a product (for example measured in market share or number of users)
- ☐ The intended use of a product (such as for the provision of health services, as an industrial control system or in a safety context)
- ☑ The safety risk associated with a product
- ☐ Other (please specify below)
- ☐ Don’t know / no opinion

Please elaborate

1000 character(s) maximum

The digital development in finance is often done in a way where a non-digital service is replaced by a digital version. Therefore, most of the digital tools and services in finance are not dealing with a new service, but rather in a new way. A good starting point when discussing potential regulation on digital products in finnace is to go by the rule “same risk – same regulation”.

Q18b: Who should determine the risk associated with a product and, as a result, its risk categorisation? *(multiple answers are possible)*

- ☐ The manufacturer
- ☐ A competent authority
- ☐ An independent body responsible for verifying compliance with the cybersecurity requirements
- ☐ Legislation
- ☐ Other (please specify below)
- ☑ Don’t know / no opinion

Please elaborate

1000 character(s) maximum

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	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	○	○	○	○	○	◉

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?

- ○ Yes
- ○ No

- [x] Don't know

Please elaborate

1000 character(s) maximum

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	○	○	○	◉	○
Horizontal cybersecurity requirements for digital products would increase awareness of users when it comes to cyber risks	○	○	◉	○	○
Horizontal cybersecurity requirements for digital products would enhance and ensure a consistently high level of the security of digital products and ancillary services	○	○	◉	○	○
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	○	○	○	◉	○

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
- ◉ Don't know / no opinion

Please elaborate

1000 character(s) maximum

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	Don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors	○	○	○	○	○	◉
Further voluntary European cybersecurity certification schemes for digital products and services	○	○	◉	○	○	○
EU public procurement guidelines taking into account cybersecurity requirements	○	○	○	○	○	◉
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)	○	○	◉	○	○	○

Introducing mandatory horizontal cybersecurity requirements for hardware products	○	○	○	○	○	◉
Introducing mandatory horizontal cybersecurity requirements for software products	○	○	○	○	○	◉

Please elaborate your answer, by quantifying the costs if possible

1000 character(s) maximum

NFU sees an enormous need for training, competence development and resources for financial employees to be able to measure up with the digital development in finance and to be able to keep up with and address cybersecurity risks. We can't stress enough the need for competence and learning on issues such as cybersecurity, data privacy and compliance. NFU and its member unions see a development where many financial employees struggle with keeping up with the digital development, something that can become a cyber risk. Companies have an important role to provide this training and accurate resources for financial employees.

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	Don't know / no opinion
Subject small and medium-sized companies to the same obligations as larger companies	○	○	○	◉	○	○
Introduce simplified procedures to demonstrate conformity for small companies and individual entrepreneurs	○	◉	○	○	○	○

Which other approaches could ensure proportionate obligations vis-à-vis small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs?

1000 character(s) maximum

It is always important to stress and secure a level playing field between larger companies and SME's. Even so, we belive that there should be same rules applied to all actors, but rather that smaller actors are provided support in complying with the rules.

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	Don't know / no opinion
Mandatory cybersecurity requirements will put smaller hardware manufacturers and software developers at a disadvantage compared with larger competitors	○	○	○	○	○	◉
Mandatory cybersecurity requirements will put EU manufacturers and software developers at a disadvantage on the non-EU markets compared to non-EU 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	Don't know / no opinion
Horizontal cybersecurity requirements for digital products would enhance protection of privacy and personal data	○	○	○	○	◉	○
Horizontal cybersecurity requirements for digital products would ensure a high level of consumer protection	○	○	○	○	◉	○

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 character(s) maximum

Final feedback

Please upload your file

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

1951d66b-4572-4e0f-a881-c093b0dc4d5c/NFU_Input_Cybersecurity.pdf

Final comments

We have added our general input to cybersecurity under files.

Contact

Contact Form