

# ASSESSING THE ECONOMIC IMPACT OF EU INITIATIVES ON CYBERSECURITY

12 JULY 2023



# Contents

Executive summary	4
<b>1 Introduction</b>	<b>7</b>
<b>2 Governments continue to develop their cyber security regulation to mitigate risk</b>	<b>8</b>
2.1 Cybersecurity threats are increasing across Europe	8
2.2 Policy makers are responding to the rise in cyber threats	9
2.2.1 The directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)	10
2.2.2 Cyber Resilience Act (CRA)	11
2.2.3 Member State “vendor screening” laws	13
2.3 The wider policy context underpinning cyber security policy and legislation	14
2.4 The importance of understanding the costs of cyber security legislation	17
<b>3 Compliance costs for businesses and impact on downstream prices</b>	<b>19</b>
3.1 Estimated cost of implementing NIS2	19
3.2 Costs to businesses of apply cybersecurity regulation	22
3.3 Incremental costs for businesses to implement NIS2	23
3.3.1 Larger firms in sectors are likely to have higher costs	23
3.3.2 Firms with higher risks will have higher costs	23
3.3.3 Firms that already are within scope of NIS will already have capacity to undertake some of NIS2’s requirements	23
3.3.4 Firms will have varying current standards of cybersecurity	24
3.4 The increase in costs will affect downstream prices	24
<b>4 Cybersecurity regulations will have implications on trade across the EU</b>	<b>26</b>
4.1 Introduction	26
4.2 Compliance costs	27
4.3 Vendor screening laws	28
4.4 Modelling approach	29

4.4.1	Compliance costs	29
4.4.2	Vendor screening	30
4.5	Results and commentary	31
4.5.1	Overall impacts	31
4.5.2	Sectoral impacts	32
4.5.3	Impact on EU GDP	32
4.5.4	Conclusions	33
<b>5</b>	<b>The resource costs for monitoring agencies to implement cybersecurity regulations</b>	<b>34</b>
5.1	Introduction	34
5.2	There is variation in the regulatory capacity of monitoring authorities across the EU	34
5.3	NIS2 and other cyber regulations will impose costs on monitoring authorities	35
5.4	Implications for monitoring authorities	37
5.4.1	Non-technical criteria	38
5.4.2	Lack of transparency in application of cyber laws	38
<b>6</b>	<b>Cybersecurity regulations can impact innovation</b>	<b>39</b>
6.1	Introduction	39
6.2	Discriminatory cybersecurity trade measures such as vendor screening can reduce innovation	39
6.3	Unclear regulatory policies can reduce innovation	40
6.4	The CRA could affect incentives of firms to innovate	40
<b>7</b>	<b>Conclusion</b>	<b>43</b>

## Executive summary

Cyber-attacks impose substantial costs on the economy and wider society. The threat will increase further as the uptake of connected devices increases and new technologies are developed. This means that all stakeholders, including governments, businesses, and consumers, have a strong interest in combating cyber threats. Governments have therefore introduced cybersecurity policies to reduce the risks of cyber-attacks and can therefore improve consumer trust and confidence across the wider society.

However, cybersecurity regulation is costly to implement. This report has estimated the costs of applying the recent EU cybersecurity regulation to illustrate the scale and types of costs that can be incurred by businesses, end-users and the wider economy.

- **Cybersecurity regulation can affect the costs of doing business, which in turn can affect the costs of trade.** The EU has developed a suite of laws and regulations to manage cybersecurity threats, though there is a degree of regulatory divergence within the EU. This is because member states have some discretion to implement the EU Directives into their country specific cybersecurity regulations; and some member states have implemented stricter measures than those envisaged by the EU (such as vendor screening in some sectors). These “discriminatory” barriers to trade will affect the willingness and incentives of firms to invest and supply products and services in the EU. Trade barriers are further increased when they are applied in a way that is non-transparent and arbitrary since it increases the degree of uncertainty for firms that wish to trade in the EU. This report estimates that imports would be **€13.4 billion** lower and exports **€19.4 billion** lower in real terms due to the introduction of discriminatory cybersecurity trade measures. This would reduce GDP by €31.2 billion in the EU.
- **Cybersecurity regulations could lead to reduced competition in concentrated markets.** In markets that rely on highly specialised equipment and/or services, the introduction of discriminatory measures which affect trade (e.g. vendor bans) could further reduce the already limited number of potential suppliers, thereby leading to the suppliers facing much less competition. This has direct and real impacts on prices paid for equipment which in turn leads to higher prices for end-users and reduces the ability of these operators to develop new innovative technologies. An example of this is the mobile telecommunications market where a recent report estimated that vendor bans for 5G equipment could increase equipment costs by **€3 billion** per year over the next decade across the EU and reduce EU GDP by **€40 billion** by 2035.
- **The additional costs for businesses across the EU to implement the cybersecurity regulations under NIS2 is estimated to be €31.2 billion per year.** This relates to the additional costs for businesses to hire cybersecurity specialists (including support staff), acquire software and install hardware in order set up and maintain additional cybersecurity frameworks and processes. These **costs will feed through into retail prices** for end users to some degree and impacting a number of industries including the manufacturing sector.

- **Cybersecurity regulations imposes costs not just on suppliers but on authorities with responsibility for implementing and monitoring the regulations.** Authorities need to be properly resourced with the specialist knowledge to apply and administer the regulations. The costs of recruiting specialist IT advisors is high given that public authorities will compete with private sector suppliers for this scarce skills base. This is important as under-resourced cybersecurity agencies will not be able to have sufficient staff to undertake the complex task of administering the regulations under NIS2 and ensuring that the regulatory interventions are targeted at the actual nature of the cybersecurity risk. There is therefore a risk that poorly staffed agencies will resort to easy to implement solutions (such as vendor bans) but which can impose high costs on users.
- **Cybersecurity regulations could deter innovation.** Markets for digital devices and services rely on businesses investing a significant amount of funds in research and development. Cybersecurity regulations could disincentivise investment innovation in the EU if it adds overly restrictive processes that affect the ability of businesses to develop, test and launch new products, thereby penalising those operators that develop products within the EU versus those foreign providers that develop their products outside the EU. Ultimately suppliers may prefer to develop products and services outside the EU to avoid this risk. The introduction of discriminatory cybersecurity trade policies (e.g. vendor bans) could further reduce investment from foreign vendors as they may be prohibited from doing business within the EU due to geopolitical factors or they may no longer wish to do business within the EU due to the uncertainties that this policy will generate. This report estimates that vendor screening measures would reduce European GDP by around **€8.9 billion**.

Given the costs of implementing cybersecurity measures it is essential that policy makers carefully design their cybersecurity policies to appropriately manage the trade-off between the costs and benefits. In this context of broad based support for the need to combat cyber threats, there is a risk that policies are unduly influenced by unconnected (or at least subsidiary) objectives leading to a policy design that may impose unnecessary costs on companies and consumers that are not (directly) related to the main objective of reducing cybersecurity threats. Policy makers may find it easier to implement their geopolitical goals, or trade policy objectives, when disguised as “cybersecurity” measures. However, this would mean that end-users may ultimately bear higher costs than necessary to address the cyber-threats.

As Member States implement the EU cybersecurity directives in the coming two years, they should be guided by the following principles to ensure that the costs of regulation are proportionate to the risks, and avoidable costs are minimised.

- **Clear and transparent** – Member States should set out the updated cybersecurity obligations and who these apply to in a clear and transparent way. Businesses should understand ex ante what is required of them to meet specified risk criteria. This will help to reduce business uncertainty which can hinder the degree of innovation and the performance of businesses.

## ASSESSING THE ECONOMIC IMPACT OF EU INITIATIVES ON CYBERSECURITY

- **Consistent** – The EU should ensure that Member States implement cybersecurity regulation in a consistent way across the EU. Inconsistent regulation reduces the incentives to invest and trade across borders and adds costs.
- **Proportionate** – Member States should only introduce cybersecurity regulations that are well-targeted at the specific risks to avoid adding an unnecessary burden onto those entities that have to comply with these regulations. Firms should be able to address any identified risk in a proportionate way, rather than being restricted from supplying in an arbitrary manner.
- **Non-discriminatory** – Member States should avoid cybersecurity regulations that are discriminatory to avoid distorting competition to the detriment of businesses and consumers. Cybersecurity regulations should be applied in a non-discriminatory way to all suppliers.
- **Technical** – Member States should introduce cybersecurity measures that focus on technical cybersecurity risks. Rules which are not focused on identifying and mitigating technical cyber-risks are likely to be inefficient (excluding firms that pose a low risk, adding unnecessary costs to firms, and creating economic frictions which reduce trade).

# 1 Introduction

Governments, businesses and consumers across the EU agree that strong cybersecurity regulations to manage cyber threats benefit all. However, cybersecurity regulations are costly to implement as businesses have to incur additional costs to strengthen their internal processes while monitoring authorities have to incur additional costs to oversee and administer these regulations. Some cybersecurity regulations can impede the process of doing business which adds cost, time and risk to business transactions.

This study has been commissioned by Huawei to contribute to the discussion on the appropriate and proportionate approach to implementing cybersecurity policies. It estimates the cost of implementing the newly proposed cybersecurity regulations under the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)<sup>1</sup>.

As Member States implement the EU cybersecurity Directives, this study can support policy makers when developing and implementing their country specific cybersecurity laws.

The rest of this report is structured as follows:

- Section 2 describes the policy context for cyber security laws;
- Section 3 estimates the resource costs of implementing NIS2;
- Section 4 estimates the impact of NIS2 on trade with, and within, the EU;
- Section 5 estimates the resource costs for monitoring authorities to implement NIS2;
- Section 6 discusses the how regulations can affect innovation; and,
- Section 7 concludes.

---

<sup>1</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).

## 2 Governments continue to develop their cyber security regulation to mitigate risk

### 2.1 Cybersecurity threats are increasing across Europe

Policy makers in Europe and across the world are responding to a rise in cybersecurity threats. The frequency of cyber-attacks across the world rose by 15% between 2020-2021<sup>2</sup> and this upwards trend is expected to continue into the future as more technologies are developed and more connected devices are used by individuals and organisations.

Cyber-attacks are committed with the intention to obtain unauthorised access to systems and networks, or with the intention to destroy or steal confidential information. These attacks can be untargeted, which involves indiscriminately targeting a large number of devices or services, or targeted, which singles out organisations due to a specific interest in their systems and/or operations.<sup>3</sup>

Cyber-attacks can impose substantial costs on organisations and the wider society in Europe and across the world. For example, the global cost of cybercrime was estimated to be €5.5 trillion in 2021<sup>4</sup> while another report by the World Economic Forum<sup>5</sup> estimated that the average cost of a cyber breach for a company was \$3.6 million in 2022.

The following Figure shows some of the most common types of cyber-attacks.<sup>6</sup>

#### Global cost of cyber attacks

---

**€5.5 TRILLION P/A**

---

*2021 - CYBERSECURITY VENTURES*

<sup>2</sup> See [https://thoughtlabgroup.com/wp-content/uploads/2022/05/Cybersecurity-Solutions-for-a-Riskier-World-eBook\\_FINAL-2-1.pdf](https://thoughtlabgroup.com/wp-content/uploads/2022/05/Cybersecurity-Solutions-for-a-Riskier-World-eBook_FINAL-2-1.pdf)

<sup>3</sup> See <https://www.ncsc.gov.uk/information/how-cyber-attacks-work>. Targeted cyber-attacks are generally more damaging as these attacks will be modified and designed to attack specific aspects of a system or network







<sup>4</sup> See <https://www.weforum.org/agenda/2022/09/new-european-union-cybersecurity-proposal-takes-aim-at-cybercrimes/>

<sup>5</sup> See [https://www3.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2022.pdf](https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf)

<sup>6</sup> See <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>



Figure 1 Types of cyber-attacks

	<b>Ransomware</b>	These take control of assets and demand a ransom for the return of the asset's availability
	<b>Malware</b>	These install malicious software to gain unauthorised access that will negatively affect the system
	<b>Social engineering</b>	These are designed to exploit human error or behaviour to obtain access – e.g. phishing, impersonation etc
	<b>Threats against data</b>	These target sources of data with the aim of gaining unauthorised access and disclosure
	<b>Threats against availability</b>	These include attacks that restrict access to IT systems and data (DDoS) or restrict access to the internet
	<b>Supply chain attacks</b>	These attacks target the both the organisation and their suppliers

Therefore, there is a consensus among all public and private stakeholders that there is a need to ensure that network and information systems are secure and resilient to potential cybersecurity threats.

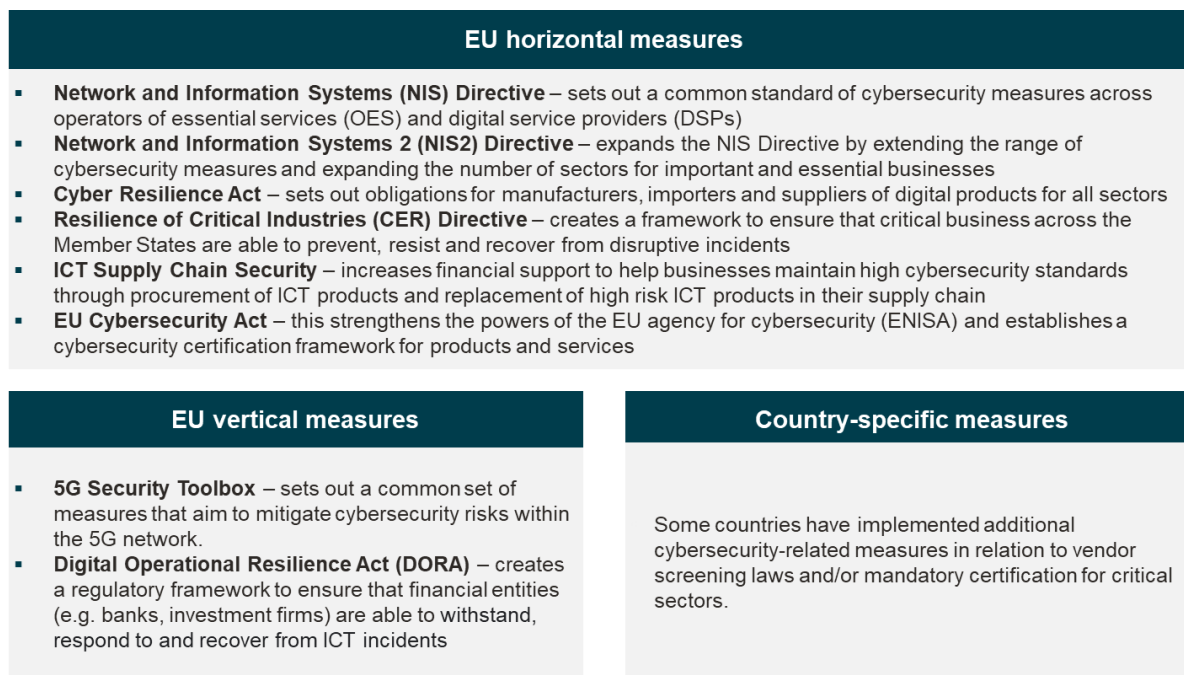
- **Governments** will want to strengthen cybersecurity standards across the industry in order to protect businesses / consumers and prevent any major disruption to the overall economy;
- **Businesses** will want to implement strong cybersecurity measures in order to protect their reputation and prevent any major disruption or financial costs that result from a cybersecurity breach; and
- **Consumers** will want governments and business to implement strong cybersecurity measures in order to prevent the loss of privacy and any major disruption of financial costs that result from a cybersecurity breach.

## 2.2 Policy makers are responding to the rise in cyber threats

Given the consequences of cyber-attacks, the EU has introduced a broad suite of interlinked cybersecurity policies, including directives, that aim to safeguard consumers, businesses and public organisations from the risk and negative consequences of cyber-attacks. These cybersecurity policies can set horizontal measures across a range of sectors, vertical

measures across specific sectors and countries can further implement their own country-specific cybersecurity policies.<sup>7</sup> Some examples of policies within each category are illustrated in Figure 2 below.

**Figure 2 Cybersecurity policies across Europe**



### 2.2.1 The directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

The NIS2 Directive has been adopted, which aims to strengthen the existing framework under the NIS Directive. NIS2 modified and expanded sectors within the scope of the NIS Directive.

The NIS2 Directive applies a risk based approach to managing cybersecurity where firms within scope self-assess their cyber-risks and implement measures accordingly. Specifically, the NIS2 Directive introduced the following:

- **Enhanced measures** – NIS2 introduced new cybersecurity measures for businesses to implement (e.g. incident response and crisis management measures) and expanded the focus of these regulations (e.g. making specific requirements on vulnerability management, audit, cybersecurity risk management processes, cybersecurity training, encryption, information security policies, the use of multi-factor authentication or other

<sup>7</sup> There are also a range of other related policies such as the General Data Protection Regulation (GDPR).

secure authentication). NIS2 also requires entities to implement cybersecurity risk mitigation requirements related to third party supplier / service.

- **Administrative actions** – NIS2 imposed a list of administrative actions, including fines for breaching cyber security management and reporting obligations.
- **Increased sector scope** – The original NIS Directive, defined sectors as “operators of essential services” (OESs) and “digital services providers” (DSPs). The scope of NIS2 now classifies firms as either ‘essential’ or ‘important’ entities, with the definition being dependent on the organisation’s criticality in terms of the economy and society. NIS2 increased the number of sectors that are subjected to cybersecurity regulations and these new sectors include waste water, manufacturing, food production, digital providers and research organisations among other sectors.
- **Improved cooperation between Member States** – NIS2 required the creation of a European Cyber Crisis Liaison Organisation Network (CyCLONe) to enable coordinated management of large-scale incidents at an EU level, and the establishment of a Cooperation Group that supports strategic cooperation and facilitates increased information sharing between Member States.

### 2.2.2 Cyber Resilience Act (CRA)

The EC has proposed the Cyber Resilience Act (CRA) which aims to create conditions for the secure development of products with digital elements irrespective of where the products are manufactured. Specifically, the CRA proposes to impose cybersecurity obligations on manufacturers, importers and distributors of digital products across all sectors.<sup>8</sup> These obligations concern:

- the design, development and production of products in such a way that they ensure an appropriate level of cybersecurity based on the risks;
- the development of products without any known exploitable vulnerabilities;
- the protection of the confidentiality and integrity of stored, transmitted or otherwise processed data;
- the processing of data that is adequate, relevant and limited to what is necessary in relation to the intended use of the product;

---

<sup>8</sup> Most of the obligations fall on manufacturers who must undertake cybersecurity risk assessments to minimise the threat of cyber-attacks and to follow a set process when introducing a product onto the market (this includes the need to draw up technical documentation, carry out conformity assessments and accompany the product with clear information and instructions). Manufacturers must also notify any incidents or becoming aware of any vulnerabilities to ENISA within 24 hours. Importers must ensure that the manufacturer has complied with the obligations under the CRA before importing the product within the market. Similarly, distributors must ensure that the manufacturer and importer has complied with their obligations under the CRA before distributing the product on the market.

- ongoing (aftersales) requirements so vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users; and
- complying with specific rules for handling vulnerabilities.

The CRA defines three categories of products and imposes obligations on manufacturers of each category.

- **Class II** – these products have the highest risk rating<sup>9</sup> and manufacturers of Class II products must complete a mandatory third-party conformity assessment.
- **Class I** – these products are less risky than Class II<sup>10</sup> and manufacturers must adhere to the application of a standard or complete a third-party assessment to demonstrate conformity.
- **Unclassified or Default** – these are identified as products that do not have any specific risks, but manufacturers must still self-assess their vulnerabilities for improvement.

Figure 3 below sets out the scope of the CRA and NIS2. This study has focused on the impact of the NIS2 Directive, but the CRA will impose additional obligations and compliance costs on essential and important businesses (as defined in NIS2) that are manufacturers, importers and/or distributors of products with digital elements.<sup>11</sup> There is also a degree of overlap since NIS2 requires that suppliers within scope manage risks in their supply chain (including suppliers of digital products). The CRA imposes specific requirements on some suppliers to NIS2 sectors as Class II obligations which require suppliers to conduct specific third-party conformity assessments.

The CRA could therefore lead to measures which are duplicated between NIS2 and CRA. While the EC did recognise this issue and included provisions for the rules to be reduced or excluded in sectors where existing EU legislation may offer the same level of protection as what is envisaged under the CRA.<sup>12</sup> However, there is still some general uncertainty on which

---

<sup>9</sup> Operating systems, hypervisors and container runtime systems, public key infrastructure and digital certificate issuers, firewalls for industrial use, industrial intrusion detection/prevention systems, general purpose microprocessors, microprocessors for programmable logic controllers and secure elements, routers for industrial use, modems for industrial use, industrial switches, secure elements, hardware security modules, secure cryptoprocessors, smartcards, readers, and tokens, industrial automation & control systems intended for the use by essential entities described in NIS2, industrial internet of things devices intended for the use by essential entities described in NIS2, robot sensing and actuator components and robot controllers, and smart meters.

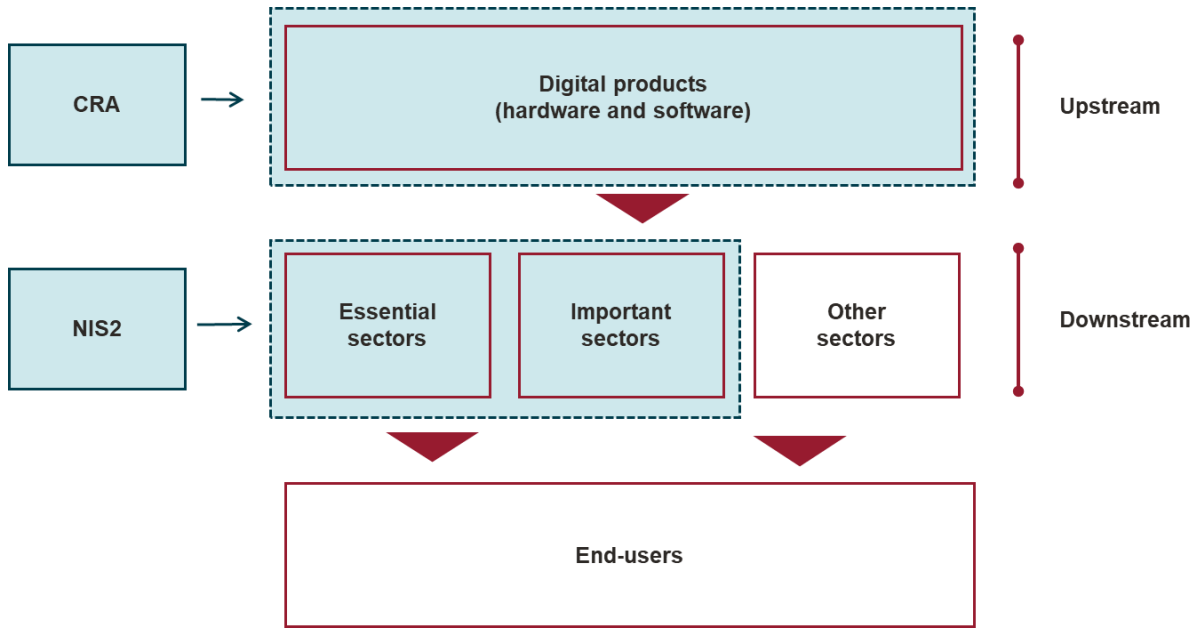
<sup>10</sup> Identity and access management software, browsers, password managers, malicious software detection, products that use virtual private networks, network management, configuration, monitoring, and resource management tools, security information and event management systems, update and patch management tools, mobile device and application management software, remote access software, physical network interfaces, microcontrollers, integrated circuits and gate arrays intended for use by essential entities described in the NIS2 Directive, operating systems, firewalls, routers, modems, microprocessors, industrial automation and control systems, and industrial IoT that are not covered by Class II of the Cyber Resilience Act.

<sup>11</sup> This study has not estimated the costs of the CRA as the CRA is still being finalised at time of writing.

<sup>12</sup> For example, the EC specifically mentioned that CRA rules will not apply to those medium sized and above entities that provide cloud computing services as these are covered by the NIS2 Directive.

sectors are covered by which regulations – this could therefore mean that there is a risk that businesses will face unnecessary compliance costs as a result of following multiple different notification and vulnerability assessment processes.

**Figure 3** The cybersecurity regulations that apply to important and essential businesses that import or distribute digital products



### 2.2.3 Member State “vendor screening” laws

Member States have implemented country specific cybersecurity laws. In some cases these regulations go beyond the requirements that are set out under the EU NIS2 framework. An illustration of the range of “screening” laws that go beyond the EU framework are summarised in Table 1 below (more information can be found within the country specific annexes).

**Table 1** Selected Member States screening laws

Country	Screening laws
Czechia	The Czech Government plans to implement a “supply chain security screening mechanism” that will allow it to screen the use of certain vendors within a range of critical sectors based on non-technical factors. The Czech Government already uses “Warnings” to screen and restrict vendors based on geo-political factors.

Country	Screening laws
France	The French Government introduced vendor selection for specific sectors. The Military Programming Law (LPM) includes a requirement for vendors to be screened before use. Similarly for 5G networks, the Law requires mobile operators to obtain approval from the Government before deployment although the Government has not made the criteria for approval public.
Germany	German cybersecurity laws allow the German Government to screen the first use of components across a range of critical sectors based on both technical and non-technical factors – the same law further allows the Government to prohibit legacy components.  The German cybersecurity law further requires manufacturer of critical components to obtain mandatory certification.
Spain	Spanish law <sup>13</sup> restricts or prohibits the use of High Risk Vendors (HRVs) to build national 5G infrastructure. The law requires the government to evaluate the risk profile of 5G vendors and may designate certain vendors as HRVs considering both: 1) their technical guarantees and their protection against attacks (e.g. compliance with certification schemes); and 2) their exposure to third-party interference (e.g. the vendor's connection with governments of other countries).  Existing cybersecurity laws further require some sectors (e.g. public administration and telecoms) to obtain mandatory certification although the list of sectors is likely to increase in the future.
Poland	The Polish Government is planning to introduce a framework to determine high risk vendors based mainly on non-technical geopolitical factors.  The Polish Government is also considering the need to introduce mandatory certification for certain sectors.

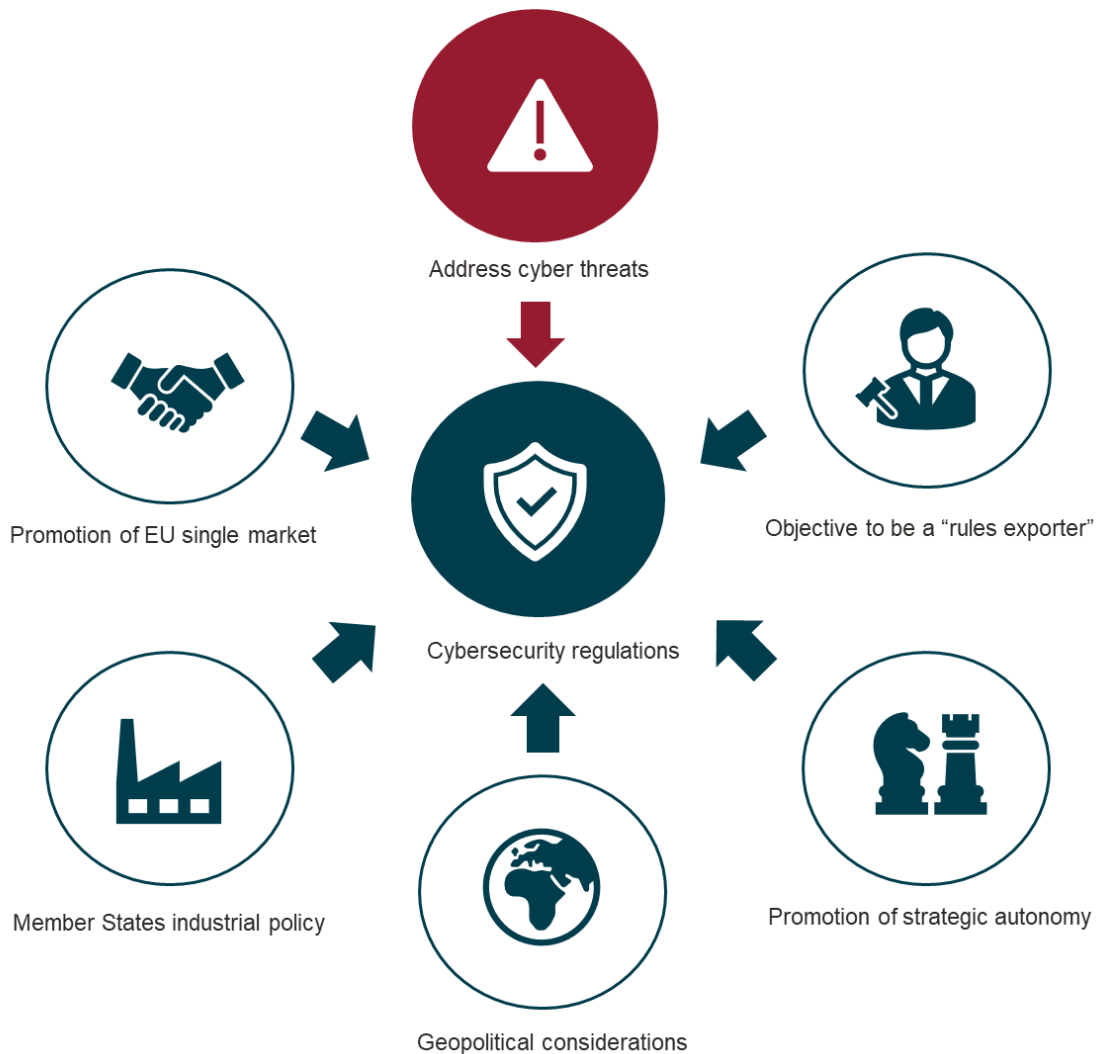
## 2.3 The wider policy context underpinning cyber security policy and legislation

Cybersecurity policy and legislation is not developed in a narrow context of managing cyber threats. Policy makers may have many different objectives in mind when designing policy. And interested parties both the private sector and within government may seek to influence the

<sup>13</sup> Royal decree-law 7/2022. A government decision designating a vendor as a HRV should set out a timeframe of at least one year for 5G operators to replace the equipment, products and services supplied by the HRV. Art. 14 royal decree-law 7/2022

design of policy to achieve their specific aims. In this context there is a risk that policies are unduly influenced by unconnected (or at least subsidiary) objectives (Figure 4).

**Figure 4 Cybersecurity obligations under wider policy objectives**



The development of cybersecurity policy could be influenced by a number of other policy objectives.

- **Promotion of the EU single market.** The EU’s internal policy goals to promote a single market and a desire for harmonised regulation. At its core a fundamental aim of the EU is to promote a single unified internal market across all 27 Member States. This implies a common set of harmonised rules around certain core areas and consistent and cooperative approach. One of the rationales for EU cyber security NIS2 was to enable a more harmonised approach to legislation.



- **The EU as a rules exporter.** In its external relations the EU benefits where it can act as a “rules exporter” or “rules setter”. Such an approach can mean that rules that it adopts are used as a template for their own laws in jurisdictions around the world. By doing so it is able to effectively set global standards on rules based approaches across certain policy areas, whether data (GDPR), product safety, consumer rights or sustainability<sup>14</sup>. It is able to achieve this not just by formal agreements (e.g. via trade agreements) but by exercising wider soft power, and by doing so it means that European firms are able to trade more easily with other countries.
- **EU and Member State geopolitical goals.** Shifts in the geopolitical landscape can influence EU / national policy. In the last decade there have been a number of shifts in the geopolitical landscape which have had profound effects on the direction of EU policy making. The US’s more assertive approach to trade ushered in under the Trump administration shaped EU policy on trade. And more recently the war in Ukraine has clearly affected the EU security, trade and energy policy. These trends potentially might imply a retreat from a rules based approach to trade to one more influenced by national priorities.
- **Strategic autonomy.** The EU has a policy to promote “strategic autonomy”<sup>15</sup> to build internal capacity and reduce reliance on external suppliers in key sectors. It implies that the EU should be able to act independently in matters of defence, trade and digital technologies.
- **Industrial policy goals.** More generally industrial policy whether practised at the EU level or Member State level can shape policy. Industrial policy promotes active intervention in sectors to promote economic objectives, whether to boost skills, employment opportunity or environmental goals. However, some forms of industrial policy can reflect protectionist pressures to promote national interests at the expense of the application of common trade rules underpinned by the WTO.

Therefore, policy makers have created cybersecurity rules in this wider policy context. Some of these objectives support a rules based approach identifying and mitigating cyber threats. For example the objective to apply harmonised rules across the EU, and seeking to be a

---

<sup>14</sup> For example in relation to the CRA the European Commission noted that “[the CRA] will impact not only the European Union. This will change the rules of the game globally, one way or another. Because they will copy us or because they will not have the tools to abide by our rules. This is good not only for the level of cybersecurity but for the competitiveness of Europe,” Lorena Boix Alonso, the director of the Commission’s department in charge of cybersecurity. See: <https://www.euractiv.com/section/cybersecurity/news/commission-expects-to-set-the-worlds-cybersecurity-standards-for-connected-devices/>

<sup>15</sup> The European Commission (EC) defines strategic autonomy as “the EU’s ability to make its own choices and shape the world around it through leadership and engagement, reflecting its strategic interests and values.” European Commission (2021), Trade Policy Review – An Open, Sustainable and Assertive Trade Policy, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, p.8



“rules” exporter which sets standards internationally both imply using a technical, risk based approach to identifying and mitigating cyber threats.

However, given the broad acceptance of the need for cybersecurity regulation, there is a risk that policy makers may find it easier to implement their geopolitical goals, trade policy objectives, or even protectionism, when disguised as “cybersecurity” measures. But poorly targeted and designed cyber security regulation will impose costs on end users.

### 2.4 The importance of understanding the costs of cyber security legislation

Member States will soon start implementing the NIS2 Directive. These regulations will strengthen the ability of public and private stakeholders to identify and mitigate the risk of cyber-attacks. However, these regulations can also lead to higher costs for businesses and the wider economy as it can affect compliance costs, downstream prices, trade and innovation. This is especially the case if Member States implement their geopolitical goals, trade policy objectives, or even protectionism, when disguised as “cybersecurity” measures. It is therefore important for policy makers to understand the potential implications of these other objectives.

The report has identified five types of costs that will result from cyber security regulations.

- **The costs for businesses across the EU to implement enhanced cybersecurity measures.** This relates to the additional costs for businesses to hire cybersecurity specialists (including support staff), acquire software and install hardware in order set up and maintain additional cybersecurity frameworks and processes (Section 3).
- **Cybersecurity regulation can affect the costs of doing business, which in turn can affect the costs of trade.** Furthermore, some cybersecurity regulations explicitly impose discriminatory regulations on non-EU firms. These “discriminatory” barriers to trade will affect the willingness and incentives of firms to want to invest in, and supply products and services in the EU (Section 4).
- **Cybersecurity regulations could lead to reduced competition in concentrated markets.** In markets that rely on highly specialised equipment and/or services, vendor bans will mean that the already limited number of service and equipment suppliers will face much less competition. This has direct and real impacts on prices paid for equipment which in turn leads to higher prices for end-users and reduces the ability of these operators to develop new innovative technologies.
- **Cybersecurity regulations imposes costs not just on suppliers but on authorities with responsibility for implementing and monitoring the regulations.** Authorities need to be properly resourced with the specialist knowledge to apply and administer the regulations (Section 5).
- **Cybersecurity regulations could deter innovation.** Markets for digital devices and services rely on businesses investing a significant amount of funds in research and development. However, the introduction of any potential discriminatory cybersecurity

trade measure could reduce investment from foreign vendors as they may be prohibited from doing business in the EU (due to factors that are unrelated to cybersecurity) and they may also be less willing to invest in the EU due to the uncertainties that this policy could generate (Section 6).

### 3 Compliance costs for businesses and impact on downstream prices

Cybersecurity regulations impose direct costs on businesses who have to comply with the regulation. This section presents estimates of the scale of costs to implement NIS2 for EU businesses.

#### 3.1 Estimated cost of implementing NIS2

The direct costs of implementing the regulation on firms across the EU is **€31.2 billion** per year representing **0.31%** of total turnover across all of the sectors that are affected by the NIS2 Directive. The impact of those sectors already regulated under NIS is €1.3 billion per year (0.20% of total sector turnover), while the increase for the sectors within scope of NIS2 is €29.9 billion per year (0.32% of total revenue). This represents a large increase in costs given that the EC estimated that average ICT security spending as a percentage of turnover was 0.52% in 2020.<sup>16</sup> This is likely to be in addition to other data regulation compliance costs (such as those associated with GDPR to protect user data and privacy).<sup>17</sup> It is important to note that these costs reflect salaries at the time of writing so this will likely increase over time due to inflationary pressures.

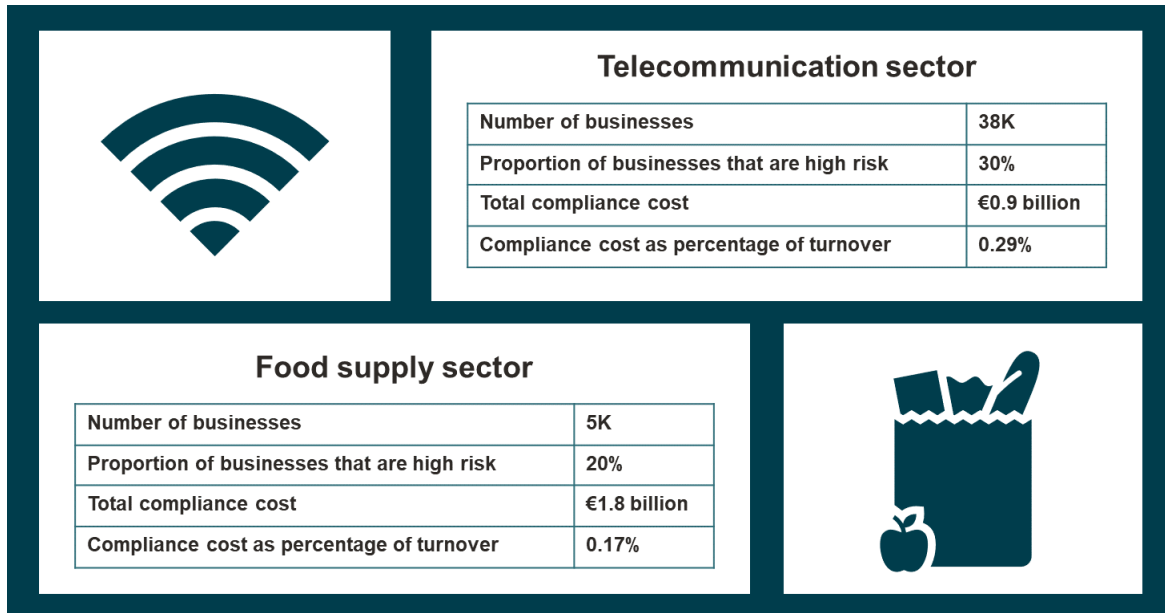
The incremental costs vary significantly across the sectors affected by the NIS2 Directive as some sectors (e.g. telecommunication) face a much larger increase in compliance costs compared to others (e.g. food production), see Figure 5 below.

---

<sup>16</sup> See Impact Assessment Part 2, <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union>

<sup>17</sup> Some studies have put the direct compliance cost to implement the EU GDPR regulation at €6.9bn. Based on a survey of large US multinational businesses. Some of these costs reflected one off costs. Source: <https://www.cpomagazine.com/data-protection/global-500-faces-gdpr-compliance-costs-of-7-8-billion/>

Figure 5 Example of costs within two sectors

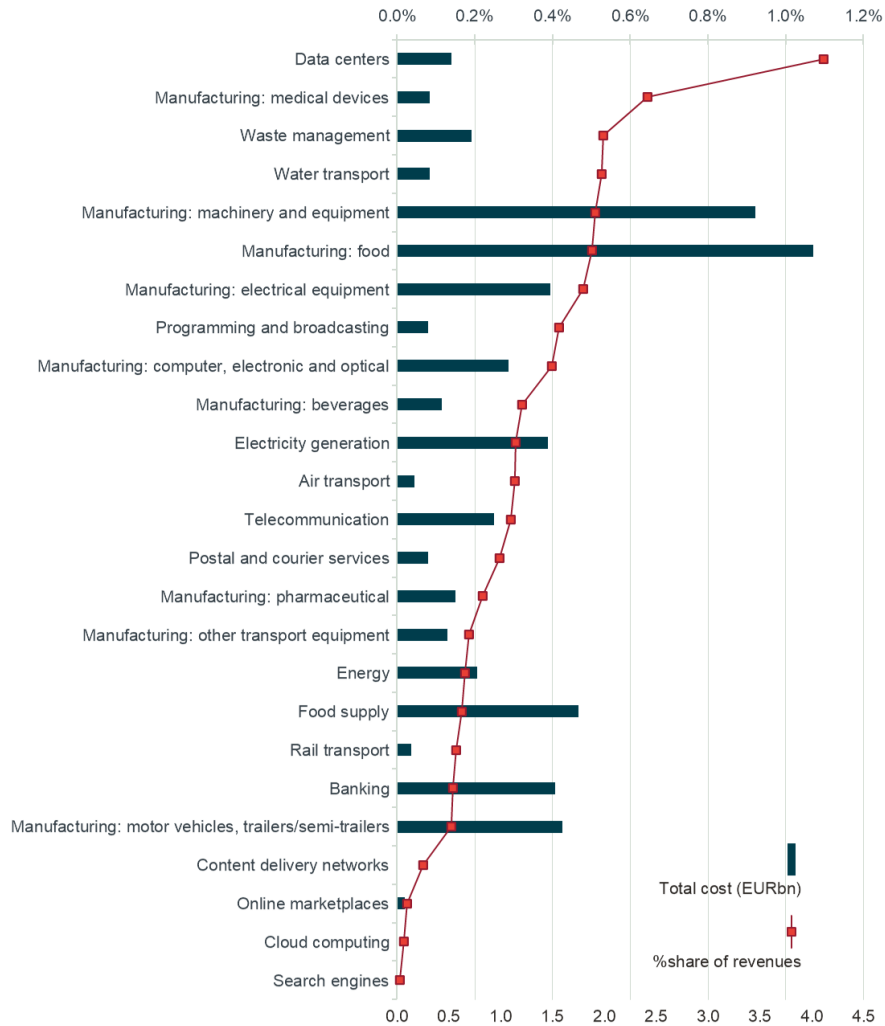


Source: Frontier Economics

Note: Selected sectors with simplified names. The full name in NIS2 of these sectors are, respectively: “Providers of electronic communications networks or of publicly available electronic communications services: Telecom” and “Food supply”

The difference in the scale of costs between sectors is driven the differences in the risk profile between sectors in risk profile and the distribution of entities with different size.

Figure 6 Compliance cost of NIS2 by sector

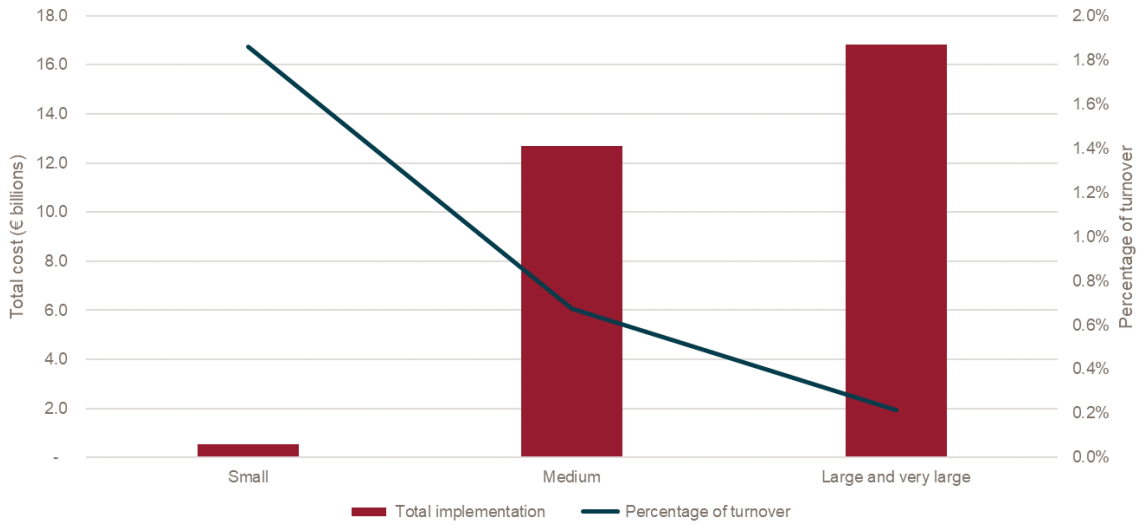


Source: Frontier Economics

Note: Results presented for a sub-set of sectors affected by NIS2

The incremental costs will also vary significantly across different sizes of businesses as smaller businesses will typically face a much larger burden relative to their total revenue than larger businesses. See Figure 7 below.

**Figure 7 Incremental cost by firm size**



Source: Frontier Economics

Note: Small business have <50 employees; Medium businesses have between 50 and 249 employees; Large and very large businesses have more than 250 employees

### 3.2 Costs to businesses of apply cybersecurity regulation

Cybersecurity regulations will lead to an increase in resource costs as businesses will need to obtain appropriate cybersecurity certification<sup>18</sup> and to strengthen their internal cybersecurity frameworks and systems. These costs are summarised in Table 2 below.

**Table 2 Types of costs for firms to implement NIS2<sup>19</sup>**

Type of costs	Description
Staff	Businesses will need to hire additional information security, business continuity and IT security staff in order to manage their internal information security management systems, business continuity management systems, and supplier risk management process and information security platforms. ENISA reported that spending on personnel represented the largest proportion of ICT spending across businesses in 2020. <sup>20</sup>

<sup>18</sup> Businesses will need to obtain appropriate international cybersecurity certification. Specifically, these relate to the need to obtain certification for information security management under ISO 27001, and security and resilience under ISO 22301. See <https://www.iso.org/isoiec-27001-information-security.html> and <https://www.iso.org/standard/75106.html>

<sup>19</sup> Other costs will also need to be considered as businesses will face higher employment related expenses (such as higher employer contributions to pensions and social security as a result of the additional staff) and higher overhead costs to support and accommodate the additional staff (such as higher accommodation, heating and electricity costs).

<sup>20</sup> See <https://www.enisa.europa.eu/publications/nis-investments-2021>

Type of costs	Description
Additional services	Businesses will need to hire additional support staff (such as legal) and seek out external support (e.g. advisory and outsourcing) to support the functions of cybersecurity staff above.
Software	Businesses will need to purchase additional software / tools to scan for vulnerabilities, conduct technical security reviews, train software developers and encrypt sensitive data. ENISA reported that spending on hardware was the second largest category for ICT spending in 2020.
Hardware	Businesses will need to install additional hardware to administer and support their internal cybersecurity frameworks, systems and processes. These could include spending on firewalls, cabling, security gateways, security appliances, security toolset platforms etc.

Source: *Frontier Economics and URM*

### 3.3 Incremental costs for businesses to implement NIS2

Not all affected firms will face the same costs to implement NIS2. Costs will vary for at least the following four reasons.

#### 3.3.1 Larger firms in sectors are likely to have higher costs

The costs incurred will vary by the size of the business. This can be for a number of reasons: because larger businesses will typically require more staff, and staff drive some cyber security costs; larger firms will have more systems to monitor and manage risks for; larger firms may have higher volumes of data, and a larger portfolio of products and services to monitor; and larger firms will have to address risks from a larger number of suppliers. This implies that as firms grow, so their cyber security costs will grow.

#### 3.3.2 Firms with higher risks will have higher costs

NIS2 is based on firms' self-assessment of their risks. The compliance costs will vary based on the cyber security risk of the sector. Some sectors (such as health and finance) may need to invest more on cybersecurity due to their sensitive nature of the data gathered and the need for these sectors to be more resilient.

#### 3.3.3 Firms that already are within scope of NIS will already have capacity to undertake some of NIS2's requirements

The exact scale of costs will vary for businesses depending on whether they are already regulated under the NIS Directive or whether they are new businesses that are included within the NIS2 Directive.

Businesses that are regulated by the NIS Directive should already have incident management processes in place which enables these businesses to detect, respond to, recover from and report incidents, near misses and breaches. This means these businesses will only need to incur the additional costs of introducing measures under the expanded NIS2 Directive.

Businesses within scope of NIS2 Directive but not NIS will have to implement the incident management processes under the NIS Directive and the wider suite of measures under the NIS2 Directive, see Section 2.2.1.

### 3.3.4 Firms will have varying current standards of cybersecurity

The NIS2 Directive has been developed based on international cybersecurity standards which means that many businesses will likely have some existing cybersecurity systems and frameworks in place. However, even allowing for this, it is likely that these cybersecurity regulations will still impose some additional costs on businesses as it is unlikely that the majority of businesses will have implemented the full suite of measures required under NIS2.

## 3.4 The increase in costs will affect downstream prices

The increase in compliance costs for the affected sectors could further have implications on downstream prices of both the affected sectors and other sectors – this is because businesses within the affected sectors may need to raise downstream prices in order to offset the rise in compliance costs while other sectors that purchase inputs from the affected sectors may need to increase downstream prices in order to offset the rise in input costs.

In general, businesses will tend to reflect changes in variable costs (i.e. costs that vary with output) within their pricing strategies. As set out above (Section 3.3.1), cybersecurity costs broadly vary in line with the size of the firm. As the firm grows so it will have to invest more in its cybersecurity resources. While costs of implementing NIS may not vary directly with output (in that one incremental unit of production leads to incremental cyber security costs) it is likely that costs will broadly scale with firm size (subject to the factors listed in Section 3.3.4).

Based on a high level analysis<sup>21</sup>, the rise in compliance costs could increase input costs by €23.4 billion for all sectors. Overall, these results show that cybersecurity regulations under NIS2 are resource intensive to implement for businesses across the affected sectors and this burden can vary across different sectors and different sizes of businesses. The costs of compliance with NIS2 could further lead to increases in downstream prices for both the affected sectors and other sectors that purchase inputs from the affected sectors.

The results above assume that there are sufficient cybersecurity and IT specialists that can be recruited by all of the affected entities and that the salaries remain unchanged. Any

---

<sup>21</sup> This analysis assumes 75% of costs are passed through to end users. The analysis uses input output tables to understand how change in costs in input sectors, feeds through to prices in output sectors. The analysis assumes no product substitution in response to price increases.



changes to these will likely have a significant effect on the results above. For example, a 25% increase on all salary costs (as a result of staff shortages) will increase total costs to €33.8 billion per year.

## 4 Cybersecurity regulations will have implications on trade across the EU

### 4.1 Introduction

This section describes the different mechanisms by which cyber regulation may impact trade, considering compliance costs and vendor exclusion aspects of the policies. A high-level description of the modelling approach is then provided, followed by results and commentary.

Cyber security regulation can have unintended (or intended) consequences on trade, which can affect economic outcomes in the EU.

- **First cyber security costs increase the costs of doing business in the EU.** This will affect EU firms serving customers in the EU ('intra-EU' or 'domestic EU' trade), EU firms serving customers outside the EU ('EU exports'), and firms outside the EU serving customers within the EU ('EU imports'). In each of these cases, increased compliance costs will raise prices relative to firms operating entirely outside the EU. This will reduce the attractiveness of firms serving the EU market, in turn reducing the EU's access to inputs from overseas, and reducing competitiveness. These costs will relate to the additional time taken to bring products to market in the EU (for example as a result of acquiring the relevant certification), the resource costs to implementing new administrative processes to ensure compliance with regulations.
- **Second some regulations may be explicitly or implicitly discriminatory** vis a vis firms operating from within, and outside the EU. There are range of regulations are in scope. Some of these may be purely technical and have equal effects on EU and foreign suppliers. At the other extreme, regulations may be explicitly and deliberately discriminatory against firms from outside the EU. There may also be intermediate cases where the regulation is not explicitly (de jure) discriminatory but amounts to a de facto discriminatory approach with firms respect to non-EU firms. For example, required technical standards may align with prevailing practice among EU firms, while being more difficult or burdensome for other firms to meet. This may or may not be deliberate.
- **Third, regulatory fragmentation across EU Member States** around cyber regulation can also disincentivise firms from considering trading with the EU. Where countries have different regulatory requirements, a firm serving numerous Member States will face multiple sets of compliance costs incurred by each different set of regulations. There may also be costs that a company incurs in order to familiarise itself with the regulatory landscape, and multiple sets of requirements may make this process more opaque and less attractive for prospective trading partners. There is already a degree of fragmentation as applied to firms, particularly in relation to vendor screening (see section 2.2.3).
- **Fourth, uncertainty as to how non-EU firms will be regulated** will also impact trade and investment decisions. This can arise both where there is uncertainty as to how policy will evolve in the future, and where understanding of how the regulatory environment

currently applies is opaque or limited. This creates a risk of investments being stranded (i.e. determined to be non-feasible after information is forthcoming), which in turn increases the expected costs of doing trade. In some countries the approach to applying regulation is not transparent.

While there is a rich causal mechanism through which these effects can act, they can be operationalised through two channels:

- *Compliance costs.* These are the additional costs that firms face in order to serve the EU market. Here the focus is on costs incurred regardless of whether the suppliers are foreign or EU-based.
- *Vendor screening laws.* This captures additional barriers that foreign providers face in order to serve the EU market. As discussed, vendor exclusion can arise both through explicit discriminatory criteria, as well as more 'objective' technical criteria that may nevertheless disproportionately affect foreign providers.

These two channels complement each other to provide a means to explore both discriminatory and non-discriminatory<sup>22</sup> mechanisms by which cyber regulation can affect trade. They are discussed in turn below.

### 4.2 Compliance costs

Compliance costs are modelled in detail earlier in the report. The calculation takes into account the different types of firm (in terms of size, sector, etc.) affected and the corresponding resource required to meet cybersecurity obligations.

Compliance costs will feed through into consumer prices. The price impact depends on the extent to which costs are fixed or variable, as well as the degree of market power. In all plausible market structures there will be some degree of cost pass-through, meaning that the compliance costs will result in some level of price impact.<sup>23</sup> At one extreme, with 'perfect competition' the impact would be passed through entirely, whereas at the other extreme, a monopolist facing fixed costs would simply bear the brunt on profits and there would be no impact. In line with the modelling approach used earlier, we assume 75% pass-through. This is a generic assumption, noting that cost and competition conditions will vary by sector, which would be a detailed question to explore in full detail.

---

<sup>22</sup> While it is certainly possible that some compliance costs could be discriminatory, we confine ourselves to the non-discriminatory costs that arise from the bottom-up modelling, to align with the evidence base established in this report. The discriminatory aspects can be considered in line with the modelling strand focused on vendor exclusion. The two will overlap, but since we have not undertaken detailed modelling of discriminatory compliance costs it is better to consider their effect within the discriminatory package devoted to vendor screening, rather than the bottom-up (non-discriminatory) cost modelling.

<sup>23</sup> This is the case across the range of imperfectly competitive markets, in which all firms face a downward sloping demand curve and in which industry demand is elastic (as profit-maximising firms always price on the elastic part of the demand curve).

These costs will be borne by firms active in the EU, whether they are serving the domestic EU market, exports overseas or imports from foreign suppliers. The compliance requirements, and hence costs, do not vary depending on whether a supplier is EU-based supplier or foreign. However, the costs do *not* affect suppliers that operate entirely outside of the EU. This brings about a 'bifurcation' of reduced trade between EU and non-EU blocs. EU compliance costs mean that non-EU firms find it less attractive serving the EU market, leaving more scope for EU firms to focus on intra-EU trade. EU businesses serving multiple markets may find it less burdensome to have operations serving only the EU, since their operations outside of the EU are also required to comply.

Compliance costs may be discriminatory or non-discriminatory. While the NIS2 Directive and CRA does not explicitly include provisions that are discriminatory although there are some articles that may encourage discrimination in favour of domestic / EU based entities.

### 4.3 Vendor screening laws

A number of European Member States have implemented and are planning to implement various forms of "vendor screening" laws that go beyond the NIS Directive, see Section 2.2.3. These policies are designed to require businesses to demonstrate that their vendors and/or suppliers meet certain cybersecurity standards before use. For example, the Czech Government is planning to implement a "Mechanism" that will allow it to screen the use of certain vendors within a range of critical sectors. This can lead to a number of concerns.

Firstly, Member States may introduce discriminatory non-technical assessments within their "vendor screening laws" where vendors could be excluded based on factors that are not related to the technical nature of the potential threat.<sup>24</sup> For example, these are cases where the assessment is based on the political and legal environment of where the supplier is based rather than the actual cybersecurity measures that the supplier has implemented.

Secondly, Member States may introduce rules that are not transparent or easily understood by the vendors, which could generate considerable commercial risks for vendors. It is also important to note that this issue may still remain in Member States where the current policy position is understood as there may be uncertainty on how these policies may evolve into the future.

Thirdly, Member States have discretion on how to implement cybersecurity regulations within their country specific laws and this has led to a significant degree of policy fragmentation across the Member States. There could again be uncertainty on how these policies may evolve into the future as some providers may in due course find themselves prohibited as a result of how the policy environment unfolds.

---

<sup>24</sup> This does not preclude the possibility that objective technical criteria that are non-discriminatory in a de jure sense could nevertheless be discriminatory in a de facto sense.

All of the above will generate considerable uncertainty and increase trade costs for foreign suppliers when serving EU markets. In turn, this will reduce competition faced by EU suppliers when serving the EU market, and reduced focus on EU exports.

The impact of vendor restriction is also substantial. This is highlighted by a recent report on 5G, which found that the exclusion of operators from the provision of 5G network equipment across 31 European countries led to an increase in investment costs by almost €3 billion per year over the next decade. The same report also found that this restriction caused a slowdown in technological innovation and economic growth with total GDP across the EU being reduced by €40 billion by 2035.<sup>25</sup>

### 4.4 Modelling approach

The overarching approach models policy shocks as changes in trade costs, which in turn affect the relative prices that consumers face, and the wages that workers earn, which are solved to give changes in trade, output and welfare. At the heart of this approach is an ‘Armington model’ in which consumers value variety of goods, but maximise utility by responding to price changes. For example in a wine context, consumers will value and consume wine from many different countries, but given budget constraints an increase in the price of French relative to Spanish wine would bring about a shift towards consumption of Spanish wine relative to French.

In this framework, policy shocks are characterised as compliance costs and vendor exclusion effects that generate price changes, and these bring about the corresponding changes in consumption and trade.

#### 4.4.1 Compliance costs

- Compliance costs are modelled on a sector level using the bottom-up framework described in previous sections. It is assumed that for any increase in costs, 75% of this is passed through as increased prices. These compliance cost shocks are applied to:
  - EU firms serving domestic national market (‘domestic trade’ e.g. German firm serving German customers);
  - EU firms serving intra-EU market (‘intra-EU trade’ e.g. German firm serving Spanish customers) ;
  - EU firms serving non-EU markets (‘extra-EU exports’, e.g. German firm serving Chinese customers);
  - Non-EU firm serving EU market (‘extra-EU imports’, e.g. Chinese firm serving German customers) ;

The shocks do not apply to:

---

<sup>25</sup> See <https://www.oxfordeconomics.com/resource/the-economic-impact-of-restricting-competition-in-5g-network-equipment/>

- Non-EU firm serving Non-EU international market ('non-EU trade', e.g. Chinese firm serving Brazilian customers);
- Non-EU firm serving own domestic market ('non-EU domestic trade', e.g. Chinese firm serving Chinese customers).

### 4.4.2 Vendor screening

Vendor screening impacts draw on 'gravity modelling', an econometric approach that estimates the responsiveness of trade flows with respect to various types of policy instrument.

To operationalise this policy instrument, we use the OECD Services Trade Restrictiveness Index (STRI), which seeks to summarise the collective impact of a large variety of measures into a single index ranging from zero (completely liberalised) to one (fully restrictive). The STRI is calculated through expert consensus, with experts attaching weights to different policy measures,<sup>26</sup> of which 'screening' is one.<sup>27</sup> Within this framework, screening is considered to be a potential barrier to foreign entry. The STRI index is maintained over a number of countries, allowing for its use as a comparison tool, including econometric analysis.

Vendor screening as described is a specific form of screening, and indeed in the OECD's calculation of the STRI, screening for cybersecurity reasons is one factor that could be taken into account in raising the level of restrictiveness captured by the STRI. It is therefore legitimate to use the OECD's STRI screening element. In the OECD STRI, screening has two components which are either set to 'on' or 'off'.<sup>28</sup> Each EU country's score range from having zero ("off") to one ("on") of each of these components switched 'on' (i.e. each component contributes 0%-50% of the full degree of restrictiveness allocated to screening).

To illustrate the impact of vendor screening, the model varies the STRI base assumption by 50% of the full screening allocation. This would illustrate a more restrictive EU Member State implementing full screening, or a non-restrictive Member State reaching medium screening. More generally, it shows the relative size of costs averted or gains forgone in relation to how these policies are applied.

Direct impacts are considered in relation to the telecoms services and computer services sectors, as these are the sectors immediately impacted. For example this captures foreign computer services providers facing barriers serving EU markets. There may also be indirect impacts, due to more general technological input shocks. For example, financial services

---

<sup>26</sup> The STRI is based on the following five categories of measures: restrictions on foreign entry, restrictions to movement of people, other discriminatory measures, barriers to competition, and regulatory transparency.

<sup>27</sup> It should be appreciated that the various measures within STRI will typically be correlated with each other (as more 'liberal' jurisdictions will be liberal across a broad range of different measures). It is therefore likely that vendor screening measures will reflect a wider range of barriers that foreign suppliers may face in this policy environment, which are related to, but not confined, to screening. This will include for example lack of transparency, regulatory uncertainty and arbitrary decision making.

<sup>28</sup> The two screening components are "Screening explicitly considers economic interests" and "Screening exists without exclusion of economic interests".

providers may find it harder trading as a result of having reduced access to computer services inputs screening inputs restrict their supply. These effects are likely to be significantly smaller than direct, but still material. However, their measurement faces some challenges using an econometric approach, so these are excluded, while noting this is conservative.

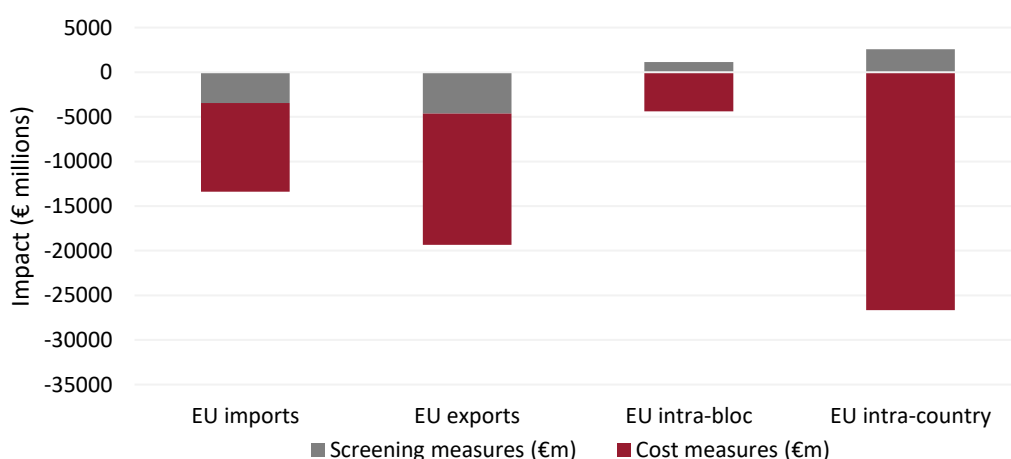
## 4.5 Results and commentary

### 4.5.1 Overall impacts

The chart below shows impacts on trade. These are broken down in terms of EU imports/exports (i.e. trade with non-EU countries), EU intra-bloc trade (trade between EU countries), and EU intra-country (production that is consumed within the same EU country).

- In total, imports are around €13.4 billion lower and exports €19.4 billion lower in real terms.
- Overall output (domestic production plus exports) is €41 billion lower.
- In terms of relative impacts of the different types of measures, around one quarter of the impact on trade (exports and imports) is due to the screening measures, with compliance costs accounting for three quarters. However, the vast majority of the net negative effect on output is due to compliance costs. The reason for this is that the vendor screening costs have a partially offsetting effect, with reduced trade inducing substitution towards EU production. By contrast, compliance costs also apply to EU domestic and intra-bloc trade, so have no offsetting effects.
- Screening measures as modelled are a relatively small proportion of the impact on trade. The measures have a positive impact on intra-EU and intra-country trade, but this is more than offset by a negative impact on trade with from outside EU.

**Figure 8 Total impacts on trade and production**



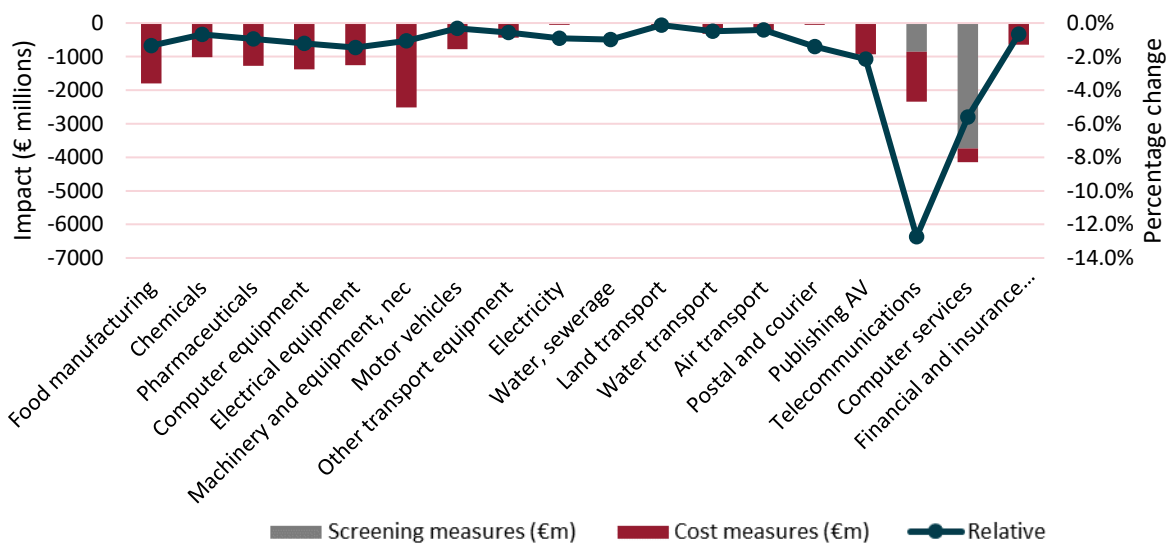
Source: Frontier Economics

### 4.5.2 Sectoral impacts

The trade impacts are shown by sector, with imports and exports for a sector occupying adjacent entries (absolute € impacts are on the left-hand side and percentage impacts on the right-hand axis).

- A range of goods sectors have large impacts in absolute terms, especially food manufacturing and miscellaneous equipment. This is driven more by the absolute size of the sectors than their relative impact. All of this is due to compliance costs.
- Telecoms and computer services are affected by both stronger compliance costs and direct screening measures. Telecoms have the largest impacts in relative terms, as they have both strong effects in terms of compliance costs, as well as in terms of screening.

**Figure 9 Impacts on exports by sector**



Source: Frontier Economics

### 4.5.3 Impact on EU GDP

Aside from trade impacts, there may also be impacts on productivity and output through a range of other channels. For example, reduced trade may inhibit transfer of technology, innovation, competition from overseas suppliers investment. An approach used by leading economists at the London School of Economics and Political Science (LSE) in their analysis



of the UK's exit from the EU<sup>29</sup> explores the relationship between trade openness and GDP. The authors explore a range of literature on the topic and in the preferred specification it is found that the elasticity of income to trade is between one-half and three quarters. Applying a mid-point assumption to the trade impacts estimated above suggests GDP reductions over the whole EU of around €31.2 billion, with the distribution of impacts similar to the chart above.

<sup>30</sup>

#### 4.5.4 Conclusions

The trade modelling approach shows the impact of compliance costs and vendor screening. Compliance costs have a more pervasive impact in that they affect domestic production, exports outside the EU, and imports, and they affect all of these. By contrast, screening measures target extra-EU imports, also affecting extra-EU exports in turn. However, they also cause some substitution towards domestic and intra-EU trade.

The compliance costs affect a broad range of sectors; even though in relative terms the impact on each is fairly small, the breadth of coverage produces large impacts in absolute terms. As modelled, vendor screening only affects telecommunications and computer services, so has a much more focused impact. There may also be wider indirect effects.

---

<sup>29</sup> Dhingra, S., H. Huang, G. Ottaviano, J. Pessoa, T. Sampson, and J. Van Reenen (2017). "The Costs and Benefits of Leaving the EU: Trade Effects." *Economic Policy*, 32(92): 651-705.  
[http://eprints.lse.ac.uk/84087/1/Sampson%20et%20al.\\_The%20costs%20and%20benefits%20of%20leaving%20the%20EU\\_Final\\_2017.pdf](http://eprints.lse.ac.uk/84087/1/Sampson%20et%20al._The%20costs%20and%20benefits%20of%20leaving%20the%20EU_Final_2017.pdf)

<sup>30</sup> Note that application of this approach already accounts for the moderating effect of EU-intra-bloc trade, as export reductions due to extra-EU exports are divided through by a larger denominator that includes intra-EU exports. As a result the GDP impacts are not identical to the trade impacts.

## 5 The resource costs for monitoring agencies to implement cybersecurity regulations

### 5.1 Introduction

The expanded scope for cybersecurity regulations under the NIS2 Directive and CRA will mean that monitoring authorities will need additional resources and capacity to administer these regulations. This will have implications on the costs of these monitoring authorities and how they develop and implement these policies. This section:

- describes the variation in institutional capacity among cyber security authorities and estimates the cost to close the capacity gap;
- estimates the cost of implementing NIS2; and,
- considers implications of the incremental requirements for cyber security authorities.

### 5.2 There is variation in the regulatory capacity of monitoring authorities across the EU

There is a degree of disparity in the existing institutional capacity of cyber security agencies to undertake appropriate monitoring and administration functions. All regulatory authorities recruit and employ highly skilled IT professionals to undertake the tasks required. In many cases such skills are scarce as the public sector are in strong competition with private sector firms for the same specialists. This can lead to insufficient institutional capacity to monitor and administer the cybersecurity regulation.

One proxy which could illustrate the variation in existing institutional capacity is the Global Cybersecurity Index (GCI).<sup>31</sup> This index measures the actions and commitment of governments to support cybersecurity across the world<sup>32</sup>.

Whilst EU Member States are leading the way in most metrics, there is a large degree of disparity across Europe. Countries such as the Germany, Estonia and Spain are ranked highly across the world while Czech Republic, Romania and Slovenia are much lower down the rankings.

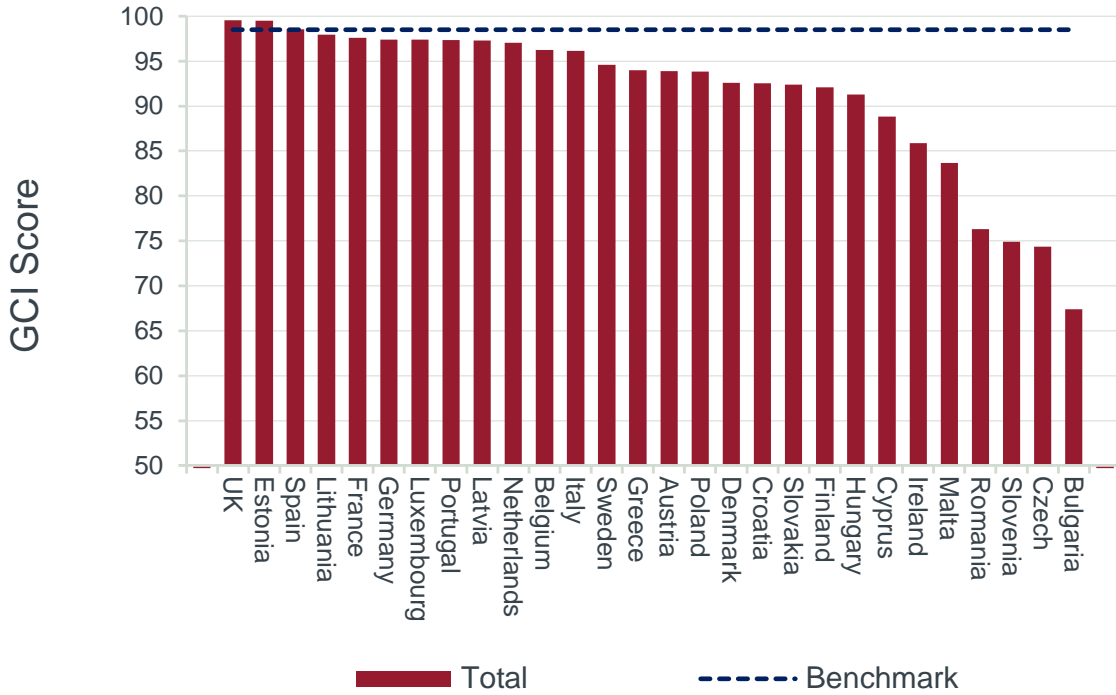
Recognising that the GCI is an imperfect measure of the capacity of monitoring agencies to implement the cybersecurity regulations, it does suggest that different monitoring agencies

<sup>31</sup> See <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

<sup>32</sup> The index is aggregated from five different measures of cybersecurity and these are the following: Legal – this measures the laws and regulations on cybercrime and cybersecurity; technical – this measures the implementation of technical capabilities through national and sector-specific agencies; organisational – this measures the national strategies and organizations implementing cybersecurity; capacity development – this measures awareness campaigns, training, education, and incentives for cybersecurity capacity development; and cooperation – this measures partnerships between agencies, firms, and countries.

may have different existing levels of capacity. This might mean that some countries will need to hire additional resources to “catch-up” to the standards of cybersecurity regulations as those that are ranked high within the table.

**Figure 10 European GCI Scores against the benchmark**



Source: Frontier Economics / URM

Data availability makes it challenging to conduct a full assessment of the institutional capacity “gap” (i.e. the incremental resources to be able to implement and administer existing regulatory functions) for different monitoring authorities. However, using GCI score of each EU country to approximate the size of the capacity gap it is possible to estimate the scale of investment that would be required to bring all institutions to the same level based on available benchmarks.

Given this approach, an indicative estimate of the additional budget required for all EU monitoring agencies to reach a high level of standard is €32.8m.

### 5.3 NIS2 and other cyber regulations will impose costs on monitoring authorities

Cybersecurity monitoring authorities have been established across the European Member States to administer cybersecurity regulations that aim to reduce and prevent cyber-attack on

public and private stakeholders. They issue cybersecurity regulations, monitor and respond to cybersecurity incidents, conduct research to improve their understanding on the evolution of cyber threats, and provide advice to consumers regarding the risks of technologies, products, services and media offerings.

The NIS2 Directive expanded the responsibilities of cybersecurity monitoring authorities as it significantly expanded the number of businesses that will need to be regulated and monitored by these authorities, see Section 2.2.1.

The NIS2 Directive further increased the range of supervisory and enforcement activities that the monitoring authorities could undertake in relation to essential businesses. These include monitoring authorities being given more powers to assess the strength of the cybersecurity frameworks of essential businesses (i.e. via on-site inspections, regular audits and requests for evidence) and powers to ensure that essential businesses become compliant (i.e. via issuing binding instructions to remedy the deficiencies and issuing warnings of non-compliance).<sup>33</sup>

For important businesses, the NIS2 Directive also similarly increased the supervisory and enforcement activities for monitoring authorities although it specified that any action must be taken ex-post.<sup>34</sup> In other words, monitoring authorities should only assess and enforce if there is a major concern or breach of the regulations.

Finally, the NIS2 Directive calls for the creation of a Cooperation Group across Europe that will work towards improving cooperation between Member States and facilitate the sharing of experience and best practice.<sup>35</sup> NIS2 Directive further requires the Cooperation Group to conduct coordinated risk assessment on critical components across the EU based on technical and non-technical factors.<sup>36</sup>

Monitoring the application and practice of cybersecurity regulation is costly as monitoring authorities will have to hire additional cybersecurity specialists and support staff in order to develop and administer these regulations in an appropriate manner. This means that monitoring authorities need to have sufficient resources in order to apply the regulations appropriately. The EC estimated that for some functions (supervisory and incident reporting), NIS2 implies a significant uplift in staff required, where as for other functions (supply chain security, enforcement, management, and cooperation) it considered an uplift in the number of staff (Table 3).<sup>37</sup>

---

<sup>33</sup> See Article 29

<sup>34</sup> See Article 30

<sup>35</sup> See Article 12

<sup>36</sup> See Article 19

<sup>37</sup> See <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union>

**Table 3** Estimated additional monitoring staff required to implement NIS2

Task	Percentage increase in staff required
Additional Supervisory tasks	20-30%
Additional incident reporting	10-15%
Supply chain security	One off 2-3 FTEs
Additional enforcement costs	1-2 legal FTEs
Additional crisis management frameworks	A two year investment of 3-4 FTEs
Cooperation Group	2-3 FTEs

Source: European Commission, *Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union*

Estimating the cost of implementing NIS2 in each EU country is not possible as there is limited information available on the existing budget and manpower allocated to cyber security is not available by country. An indicative estimate suggests collectively cybersecurity authorities would have to invest €360 million to undertake the additional responsibilities required by NIS2<sup>38</sup>.

## 5.4 Implications for monitoring authorities

NIS2 means that monitoring authorities will face an increase in costs of up to €360 million to require additional specialists to administer the expanded cybersecurity regulations. However, cybersecurity monitoring authorities may find it difficult to attract these specialists given the general shortage of IT specialists. These public bodies would be competing with private companies to hire these specialists.

There is therefore a material risk that monitoring authorities may not have sufficient quality resources to effectively administer the regulations based on the principles set out by the EC in relation to ensuring that policymaking is based on evidence, with laws needing to be simple but effective, avoiding unnecessary burdens.<sup>39</sup>

This means that monitoring authorities, given the lack of quality resources, could resort to implementing less technical and more simplistic solutions to cyber security. Instead of implementing policies based on analysing the technical details of the risk and offering opportunities for businesses to proportionately mitigate the risk, these monitoring authorities

<sup>38</sup> This assumes that the above measures lead to a 15% increase in resources consistent with the assumptions in Table 3; and assuming that investment in cybersecurity authority resources (adjusted for country GDP) was equivalent to the UK (which publishes data on staff numbers and total budget).

<sup>39</sup> See [https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation\\_en#objectives-of-the-better-regulation-agenda](https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_en#objectives-of-the-better-regulation-agenda)

may instead introduce policies that screen businesses for exclusion purposes. The lack of resources could also mean that cybersecurity policies are not set out clearly, allowing greater interpretation to monitoring authorities, therefore affecting business incentives.

#### 5.4.1 Non-technical criteria

Monitoring authorities that are not sufficiently resourced will be more likely to resort to low cost approaches to monitor and enforce regulations on the market. This can involve introducing measures and/or restrictions based on non-technical assessment as this is easier to apply and will require less resources than policies that require the monitoring authority to assess suppliers based on the technical detail and develop an approach to mitigate any identified risk. As such, this gives scope for policy makers to make decisions based on geopolitical and industrial policy goals, see Figure 4, both of which should not have a dominant influence on decision making.

This can be illustrated by the current situation in Czechia where the Czech government / cybersecurity regulator (NUKIB) is planning on introducing a “Mechanism” that aims to exclude vendors based on non-technical assessments and without providing an opportunity to the vendor to mitigate the relevant cybersecurity risk.

The introduction of non-technical assessments will lead to higher costs for end-users. This is because the exclusion of vendors and/or suppliers will reduce competition thereby leading to higher input prices for businesses, increased costs for end-users and other negative implications to the wider economy.

#### 5.4.2 Lack of transparency in application of cyber laws

There could also be a higher risk that monitoring authorities may set out policies that are unclear and non-transparent when they are under-resourced. This can be particularly problematic if under-resourced monitoring authorities were to introduce unclear and non-transparent policies in relation to the process and the criteria that the monitoring authority will use to assess the degree of risk.

This could lead to a significant increase in costs as suppliers may be less willing to enter into markets or bid for contracts in markets where the overall process is uncertain even if the supplier has a strong standard of cybersecurity. This can therefore create a similar impact to the section above as this will lead to a reduction in competition and higher prices paid by consumers.

An example in France, where 5G network operators need to submit a proposal to the Prime Minister’s office to use equipment from certain vendors before deployment, with some vendors considered riskier than others. The Prime Minister’s office then decides whether or not to grant permission depending on the sensitivity of the region in which it is deployed, with this criteria not made public. The length of the permit could differ with the operator made aware of this time period but is not allowed to communicate this to the vendor.

## 6 Cybersecurity regulations can impact innovation

### 6.1 Introduction

Innovation is the fundamental building block of economic growth. Research which expands the stock of knowledge supports new forms of technological advancement which enables economies and societies to benefit from higher incomes and new technologies. Digitally intensive sectors are particularly suited to promoting innovation as they disproportionately contribute to Research and Development (R&D), which in turn means that they disproportionately contribute to economic growth.<sup>40</sup>

However, innovation is necessarily risky and volatile as the ability of business to invest will depend on the potential returns that they could earn from R&D versus the potential costs of the investment. Innovation will further depend on the ability of businesses to dedicate funds for R&D purposes as they will have to balance the benefits of investing in R&D versus the potential benefits from committing funds for other competing purposes. This means that the design and implementation of cybersecurity regulations is important as these regulations can affect the ability of businesses to launch new products into the market and they can also affect the amount of funds that can be used by businesses for investment purposes.

In general, policy makers should avoid implementing cybersecurity regulations in a non-transparent manner as this could further increase the level of uncertainties, thereby leading to lower incentives for businesses to invest. Policy makers should also avoid implementing discriminatory cybersecurity measures (e.g. vendor bans based on non-technical factors) as this can further reduce investment from foreign vendors and increase the costs of domestic businesses.

### 6.2 Discriminatory cybersecurity trade measures such as vendor screening can reduce innovation

Markets for digital devices and services rely on businesses investing a significant amount of funds in R&D. Discriminatory cybersecurity trade measures could deter or slow down innovation as it could reduce investment from foreign vendors who are prohibited from doing business in the EU or they may no longer wish to do business within the EU.

These discriminatory cybersecurity trade measures could also reduce the number of potential suppliers thereby leading to lower competition and higher input prices, thereby further reducing the amount of funds that would be available for investment purposes. This effect will be particularly harmful for those sectors that rely on highly specialised equipment or services as

---

<sup>40</sup> For example, ICT producing sectors account for two-thirds of productivity growth in Germany, and Slovenia and just below 50% in France and the Netherlands. See <https://www.oecd.org/economy/growth/ict-investments-and-productivity-measuring-the-contribution-of-icts-to-growth.pdf>

there may already be limited supply of alternative suppliers that have invested in the necessary research and development to provide alternative inputs.

The impact on innovation on the overall economy could be illustrated by exploring the impact of vendor screening on productivity, since productivity gains are the result of investments in innovation. Vendor screening could be considered as an increase in the tariff on imports as it restricts the number of vendors, thereby leading to higher prices. Recent work by the IMF showed that a percentage point decrease in tariffs is associated with a 2% increase in economy wide productivity.<sup>41</sup> This would equate to a **reduction in European GDP of around €8.9 billion.**<sup>42</sup>

Given this, policy makers should carefully balance the need to introduce these discriminatory cybersecurity trade measures against the potential costs of these policies to innovation (and other areas such as trade, see Section 4).

### 6.3 Unclear regulatory policies can reduce innovation

Investment in innovation is inherently risky as businesses face significant uncertainties in relation to the potential returns they could earn and the likely costs that they will likely incur. Therefore, policy makers should design and implement policies in a transparent manner in order to minimise any additional uncertainties that can affect investment decisions. This is particularly the case as a recent study found that policy uncertainty lead both public and private businesses to reduce their investment across 9 European countries.<sup>43</sup>

This could also be harmful for those sectors that tend to also have a complex multi-layered supply chain of vendors as the introduction of discriminatory trade measures (based on non-technical factors) could drastically increase the level of uncertainty as these rules will require the cybersecurity authority to assess the full range of input components.

### 6.4 The CRA could affect incentives of firms to innovate

The CRA requires all digital and services products to be assessed for their cybersecurity risks. It ensures that suppliers (whether manufacturers or suppliers such as distributors or importers) assess the cybersecurity risks associated with their products and commits suppliers to remedy any problems following the sale<sup>44</sup>.

---

<sup>41</sup> See <https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Reassessing-the-Productivity-Gains-from-Trade-Liberalization-43828>

<sup>42</sup> Note that there is potential double counting between the effects of vendor screening on GDP estimated here and the trade-openness approach that was used in the next section, as both will include effects on ICT as an input into other sectors

<sup>43</sup> See <https://link.springer.com/article/10.1007/s11846-022-00603-y>

<sup>44</sup> For up to five years or otherwise during the expected product lifetime.



The CRA's objectives are clearly valuable to users of technology whether end-users or businesses that require digital inputs for complex products. It provides ongoing reassurance that digital products, services, and components are appropriately assessed for risks throughout the product lifecycle.

However, there is a risk that the Act could harm incentives to invest in innovation in the EU. The production and development process of digital devices and services is immensely complex. It necessarily involves significant investment in high value R&D, as digital firms develop, test, iterate their products and services.

Suppliers will face a number of potential risks in that could deter their investments.

First, there is a risk that the certification and approval process could be time consuming which could delay potential launch and supply of products. This will damage the investment case for undertaking innovation in the EU. This would affect not just new products but potentially could affect existing products (for example where a software update makes a sufficiently large change in the product's functionality). The acceptable standards may not be obvious to manufacturers, who will have to invest time and capital to undertake the appropriate certification. In highly dynamic markets this could add costs. These costs will be exacerbated where regulation is untransparent or even arbitrary.

Second, suppliers potentially face more open-ended liabilities to continue to monitor and maintain their products long after the initial sale for the duration of the lifecycle of the product, under threat of punishment. These costs will be factored into the business case for investing in innovation to develop new products. But these costs do not depend only on the actions of the provider, as they will depend on how the technology which could exploit vulnerabilities develops.

Third, the CRA limits how firms can engage in some forms of product testing. Many products undergo testing and evolution in the market. Products use a "soft launch" or a BETA phase where the product is supplied on a limited basis to the target users of the product. During this phased developers ask users to point out bugs, highlight possible functionality improvements, and evaluate their personal user experiences as a whole. While there is a specific exemption in the draft CRA for product testing to permit testing<sup>45</sup> this exemption is limited (in time and purpose) and suppliers may consider that it would be risky to undertake open market product testing in the same way. Firms will be concerned that legitimate forms of product testing could be deemed to infringe the CRA.

Fourth, many products and devices are provided relying in some degree on opensource software which is licensed to developers to use and build and test new products. The use of open-source software can reduce the cost of developing software, and can enable a degree

---

<sup>45</sup> CRA draft Recital 21. "In order to ensure that manufacturers can release software for testing purposes before subjecting their products to conformity assessment, Member States should not prevent the making available of unfinished software, such as alpha versions, beta versions or release candidates, as long as the version is only made available for the time necessary to test it and gather feedback."

of compatibility or interoperability between different devices using the opensource software. The CRA notes that the use of open source software is excluded from CRA where the software is not supplied on a commercial basis. However, there may be many different forms of supply of open source licensed software which might have some element of commercial activity (and hence not attract the exemption).

The impact of these restrictions will go beyond the resource costs of compliance, and are necessarily difficult to measure. Entrepreneurs must have the willingness, opportunity/motivation, and capability or capacity to innovate, and that regulation can affect all three aspects.

*According to research by the EC “Different types of regulatory approach can have different impacts on innovation typically, more prescriptive, rigid regulation can hamper innovative activity, whereas the more regulation is flexible, the more innovation can be stimulated. During the enforcement phase of regulation, the lower the costs of compliance and the administrative burdens, the more positive is the impact on innovation”<sup>46</sup>.*

However, there is a risk that these principles are not embodied in the current draft of the CRA and hence will risk innovation in the EU. In order to avoid an innovation penalty the CRA should be designed in a way that supports flexibility, enhanced transparency, promotion of information sharing, over prescriptive, inflexible requirements.

---

<sup>46</sup> European Commission (2014) How can EU Legislation Enable and/or Disable Innovation?

## 7 Conclusion

Cybersecurity measures, when designed appropriately, should enhance the strength and resilience of cybersecurity practices, thereby ensuring that businesses and consumers can benefit from a reduction in the losses and frequency of security incidents. The EU NIS2 Directive and CRA are aimed at improving the resilience of industries against cybersecurity threats across the EU and to improve coordination on cybersecurity matters between Member States.

While enhanced cyber security is welcome, policies need to be carefully designed to ensure that potential costs are proportionate to the benefits. Cybersecurity regulations could have significant implications for businesses, monitoring authorities and the wider economy in terms of downstream prices, trade and innovation. Policy makers should therefore be aware of these implications when designing and implementing their cybersecurity regulations.

- **Cybersecurity regulation can affect the costs of doing business, which in turn can affect the costs of trade.** The EU has developed a suite of law and regulation to meet manage cybersecurity threats including, though there is a degree of regulatory divergence within the EU. This is because member states have some discretion to implement EU Directives in their country specific cybersecurity regulations; and some member states have implemented stricter measures than envisaged by the EU (such as forms of vendor screening in some sectors). This report estimates that imports would be **€13.4 billion** lower and exports **€19.4 billion** lower in real terms due to the introduction of discriminatory cybersecurity trade measures.
- **Cybersecurity regulations could lead to reduced competition in concentrated markets.** This has direct and real impacts on prices paid for equipment which in turn leads to higher prices for end-users and reduces the ability of these operators to develop new innovative technologies. An example of this is the mobile telecommunications market where a recent report estimated that vendor bans for 5G equipment could increase equipment costs by **€3 billion** per year across the EU and reduce EU GDP by **€40 billion** by 2035<sup>47</sup>.
- **The additional costs for businesses across the EU to implement the cybersecurity regulations under NIS2 is estimated to be €31.2 billion per year.** This relates to the additional costs for businesses to hire cybersecurity specialist (including support staff), acquire software and install hardware in order set up and maintain additional cybersecurity frameworks and processes. These **costs will feed through into retail prices** for end users to some degree.
- **Cybersecurity regulations imposes costs not just on suppliers but on authorities with responsibility for implementing and monitoring the regulations.** Authorities

<sup>47</sup> Source: Oxford Economics. The Economic Impact of Restricting Competition in 5G Network Equipment. Under the central cost scenario, the report suggests that restricting a key supplier of 5G infrastructure in the 31 European countries would increase total investment costs by almost €3 billion per year, on average, over the next decade (in 2020 prices). <https://www.oxfordeconomics.com/resource/the-economic-impact-of-restricting-competition-in-5g-network-equipment/>

need to be properly resourced with the specialist knowledge to apply and administer the regulations. The costs of recruiting specialist IT advisors is high given that public authorities will compete with private sector suppliers for this scarce skills base. This is important as under-resourced cybersecurity agencies will not be able to have sufficient staff to undertake the complex task of administering the regulations under NIS2 and ensuring that the regulatory interventions are targeted at the actual nature of the cybersecurity risk. There is therefore a risk that poorly staffed agencies will resort to easy to implement solutions (such as vendor bans) but which can impose high costs on users.

- **Cybersecurity regulations could deter innovation.** Markets for digital devices and services rely on businesses investing a significant amount of investment in research and development. Cybersecurity regulations could disincentivise investment innovation in the EU if it adds overly restrictive processes that affect the ability of businesses to develop, test and launch new products, thereby penalising those operators that develop products within the EU versus those foreign providers that develop their products outside the EU. Ultimately suppliers may prefer to develop products and services outside the EU to avoid this risk. The introduction of discriminatory cybersecurity trade policies (e.g. vendor bans) could further reduce investment from foreign vendors as they may be prohibited from doing business within the EU due to geopolitical factors or they may no longer wish to do business within the EU due to the uncertainties that this policy will generate. This report estimates that vendor screening measures would lead to a fall in productivity equating to a reduction the EU European GDP of around **€8.9 billion**.

EU Member States have a degree of discretion in how to implement cybersecurity laws and regulations to reflect the updated NIS2 Directive (the proposed CRA is also regulation and is directly applicable). As discussed in the Annexes below, some countries have implemented frameworks that can go beyond the EU frameworks which limit the ability of firms to compete and supply digital goods and services in the EU (e.g. implementing vendor screening laws). These can have a significant negative impact on compliance costs and trade.

In order to ensure that the cybersecurity regulations are designed to mitigate risks in the most effective way, and are proportionate to the benefits they should be implemented by the Member States based on the principles highlighted in the Figure 11.

**Figure 11 Principles of implementing cybersecurity regulations**

<p><b>CLEAR AND TRANSPARENT</b></p>	<p>Member States should set out the updated cybersecurity obligations and who these apply to in a clear and transparent way. Businesses should understand ex ante what is required of them to meet specified risk criteria. This will help to reduce business uncertainty which can hinder the degree of innovation and the performance of businesses.</p>
<p><b>CONSISTENT</b></p>	<p>The EU should ensure that Member States implement cybersecurity regulations in a consistent manner across Europe. Fragmented cybersecurity regulations will reduce the incentives to invest and trade across borders, and adds costs.</p>
<p><b>PROPORTIONATE</b></p>	<p>Member States should only introduce cybersecurity regulations that are well-targeted at the specific risks to avoid adding an unnecessary burden onto those entities that have to comply with these regulations. Firms should be able to address any identified risk in a proportionate way, rather than being restricted from supplying in an arbitrary manner.</p>
<p><b>NON- DISCRIMINATORY</b></p>	<p>Member States should avoid cybersecurity regulations that are discriminatory to avoid distorting competition to the detriment of businesses and consumers. Cybersecurity regulations should be applied in a non-discriminatory way to all suppliers.</p>

Member States should avoid regulatory fragmentation unless there are justified reasons from introducing these measures.

To support the implementation of cybersecurity regulations based on all the principles above, Member States should consult on the proposed regulations with stakeholders in order to improve transparency and allow stakeholders to feed into the overall process. These consultations should also be supported by an appropriate and transparent cost benefit assessment if possible.

If these principles are applied, not only will the cybersecurity policy be designed in a way that is effective and focused on identifying and mitigating risk, but they will ensure that costs are minimised and proportionate to the risks. Such an approach would support the EU's objectives to be a standard setting rule maker around the world, and to limit harmful regulatory fragmentation.

Frontier Economics Ltd is a member of the Frontier Economics network, which consists of two separate companies based in Europe (Frontier Economics Ltd) and Australia (Frontier Economics Pty Ltd). Both companies are independently owned, and legal commitments entered into by one company do not impose any obligations on the other company in the network. All views expressed in this document are the views of Frontier Economics Ltd.

