WWW.FRONTIER-ECONOMICS.COM

IMPLICATIONS OF NEW CYBER SECURITY MEASURES IN PORTUGAL

24 APRIL 2024

Contents

frontier economics

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 (adding 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 Network and Information Security 2 Directive (NIS2) in Portugal and is part of a wider study looking at the costs of implementing cyber security measures in the EU[1].

Strong cybersecurity measures in Portugal are important, but they need to be designed carefully to avoid imposing unnecessary costs on end-users and the wider economy

Cyber-attacks impose substantial costs on the economy and wider society. This threat will increase further as the uptake of connected devices increases and new technologies are developed. This means that all stakeholders, including governments, businesses, suppliers of digital goods and services, and consumers, have a strong interest in combating cyber threats.

The European Commission has addressed the threat with a suite of proposals including the NIS2 Directive, which aims to provide a common, transparent and risk based approach to implementing cybersecurity measures across the European Member States. The NIS2 Directive extends the 2016 NIS Directive and complements other cybersecurity policies such as the Resilience of Critical Industries Directive, 5G Security Toolbox and Digital Operational Resilience Act (DORA). At the time of writing, the NIS2 Directive is currently being implemented by the Portuguese Government and other Member States into their country specific cybersecurity laws and legislation.

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. While enhanced cybersecurity measures are welcome, it is important to recognise that cybersecurity regulations can also impose substantial costs on businesses and the wider society depending on how it is implemented. This report estimates that the costs to implement the NIS2 Directive for Portugal would amount to the following:

[1] https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf

- an increase in costs for businesses of **€529 million** to implement new regulations;
- higher downstream prices for the directly affected sectors but also higher prices in other sectors;

Policy makers in Portugal have implemented cybersecurity policies that are proportionate and targeted at the technical nature of the risks. However, there is a concern that some of the recently implemented cybersecurity policies could lead to policy makers relying on non-technical factors (e.g. geopolitical factors) when assessing the cybersecurity risk of foreign vendors. This will have a negative net impact on consumers as these policies will lead to higher costs (e.g. lower competition and innovation) but it will not address nor mitigate the technical nature of the cyber-risks. This report estimates that the potential impact of vendor screening could amount to the following:

- a reduction in extra-EU exports of **€169 million** and extra-EU imports of **€37 million**; and
- a reduction in GDP of **€289 million.**

Given this, policy makers in Portugal should focus on "technical factors" when assessing the degree of risk (i.e. factors that directly relate to the technical cyber risk) as this will ensure that any regulatory action is targeted and proportionate.

Portugal has, in general, implemented cybersecurity policies in a proportionate manner but there is a concern that some of the recent policies have gone beyond the European Directives

The NIS1 directive was transposed in the Portuguese legislation through Law No. 46/2018 on August 13 by establishing a legal framework for cyberspace security. The transposition and implementation of the NIS1 directive was proportionate but there is a concern that it went beyond the directive.

In additional to this framework covering the operators of essential services and digital service providers, it also covers the Public Administrators and operators of critical infrastructures[2]. In this sense, it goes beyond the NIS1 directive by imposing the measures on additional sectors.

[2] Cuatrecasas Report: Directive (EU) 2016/1185 (NIS Directive) and Directive (EU) 2022/2555 (NIS2 Directive) : An Overview of Current Implementation

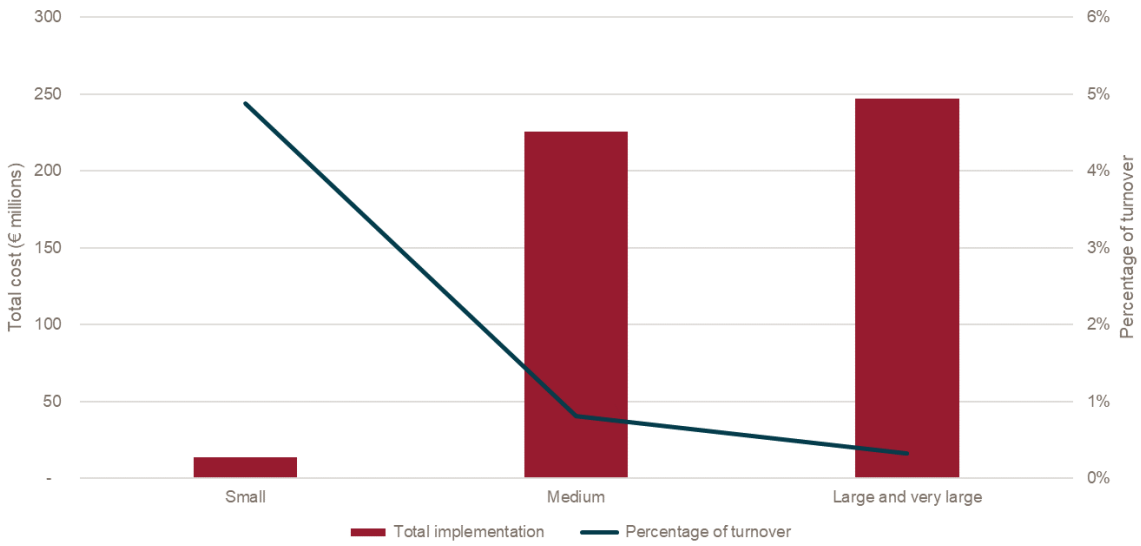
In transposing the NIS2 directive, Portuguese government should avoid "gold plating"[3]. This implies that the legislation should not impede the functioning of the EU internal market and not infringe the principle of non-discrimination under Article 18 of the TFEU.[4]

The EU Law Principles prohibit creating barriers to free movement of goods and services. In this sense, transposition of NIS2 must only restrict free movement of services in the presence of a cyber security threat.

Cybersecurity imposes direct costs on businesses affected

The cost of implementing the NIS2 Directive in Portugal is estimated to be **€529** million. Figure 1 below further shows that the NIS2 Directive will have a proportionately larger impact on smaller businesses as the implementation costs as a percentage of business turnover is higher for small businesses than for larger businesses.

Figure 1 Cost of implementing NIS2 by business size



Source: Frontier Economics

The increase in implementation 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.

[3] Gold plating refers to over extending the legislation while transposing EU directives.

[4] Cuatrecasas Report: Directive (EU) 2016/1185 (NIS Directive) and Directive (EU) 2022/2555 (NIS2 Directive) : An Overview of Current Implementation

Cybersecurity measures cause economic frictions which lead to costs

The imposition of NIS2 measures can in addition cause "frictions" in how firms trade with each other which has real costs to the economy. As discussed above, the cybersecurity measures add to the cost base of companies transacting in the EU, whether that be local firms serving the domestic market, looking to supply outside the EU, or be foreign suppliers serving the EU. In each of these cases, costs and prices will increase. However, there is no direct effect on a foreign supplier serving non-EU markets. This has potential to create a 'bifurcation' in the market, where suppliers from outside the EU find it more attractive serving non-EU markets and configure operations in that direction. With this reduction in imports from outside the EU, EU-based suppliers facing reduced competition will orientate more towards serving their 'home' market rather than non-EU markets. As a result, there is reduced trade between the EU and rest of the world with reduced benefits in terms of international competition and access to innovation and the full range of product offerings.

Furthermore, the fragmentation of cybersecurity policy *within* the EU can impose frictions on trade. In the case of NIS1, transposition gave Member States a very wide margin of discretion, which resulted in high heterogeneity in the application of the provisions, contributing to the phenomenon of fragmentation.[5] Fragmentation can affect the free movement of services within EU and impose costs on businesses. Use of technical-factors across Member States can help avoid this fragmentation.

Discriminatory cybersecurity trade measures to exclude vendors will impose substantial costs

Discriminatory policies which "screen" which firms can supply goods and services will impose costs on businesses.[6] As discussed above, there is a risk that policy makers in Portugal will use non-technical factors to screen potential vendors. This will likely have a negative net impact on consumers as these policies could lead to higher costs (e.g. lower competition and innovation) but it will not address nor mitigate the technical nature of the cyber-risks. This is especially the case as the usage of non-technical criteria will likely lead to error and inefficiency in the identification and treatment of cyber risks. Given this, policy makers in Portugal should focus on using technical factors when assessing the degree of risk as this will ensure that any regulatory action is targeted and proportionate.

[5] EY - Approach to the transposition of the NIS2 Directive in Portugal

[6] Analysis by the OECD to quantify barriers to services trade using the Services Trade Restrictiveness Index (STRI) considers the impact of screening alongside a whole raft of other measures thought to be trade-restricting, such as barriers to foreign entry, movement of labour and barriers to competition. The STRI is weighted according to a consensus of expert judgement. In various empirical literature the STRI is found to have a negative effect on trade, so that screening has a negative effect alongside these other types of restriction.

Discriminatory cybersecurity measures will increase costs of doing business within Portugal

Even where screening measures do not 'bite', they impose additional compliance costs to prospective suppliers who must engage with the screening process, and add to regulatory uncertainty. Where the uncertainty is sufficiently large, this has the potential to outright deter investment, as there is a risk that the investment costs will not be recouped, and that the project is no longer viable. Transaction costs may have a disproportionate impact where there are already transaction costs related to doing business, such as sunk costs incurred in tailoring products to meet the specific needs of local markets. Local suppliers will also face impacts as a result of building relationships and transacting with parties who may subsequently be barred. So the chilling effect of discriminatory measures will affect both foreign and domestic suppliers.

Discriminatory cybersecurity trade measures will reduce competition and lead to increased costs

Discriminatory cybersecurity trade measures will likely create "economic frictions" that negatively affect trade, reduce competition and slow down innovation. Screening policies tend to have a negative net impact on consumers. This is because these screening policies will reduce the number of suppliers and could further deter potentially acceptable foreign suppliers from operating and investing in Portugal as they may not consider it worthwhile to deal with the uncertainties and the processes. This could subsequently reduce competition and increase prices for a range of sectors (that will be additional to the costs highlighted above). These impacts can be felt in any sector where the need for specialised equipment means that there is a limited supply of vendors, whether energy, medical devices or telecommunications equipment. For example, a recent report highlighted that vendor bans on 5G equipment could increase 5G equipment cost for Portugal by **€63 million** per year over the next decade and reduce GDP by **€500 million by 2035.**[7]

Discriminatory cybersecurity trade measures can deter innovation

Markets for digital devices and services rely on businesses investing a significant amount of funds in research and development. Screening processes could deter or slow down innovation to the detriment of consumers and wider society. This is because the process could reduce investment from foreign vendors who are prohibited from doing business in Portugal or they may no longer wish to do business in Portugal due to the uncertainties that this policy will generate. Screening processes could further reduce investment from other local businesses due to higher input costs and lower competition.

This impact could be particularly harmful for certain sectors such as:

[7] See https://www.oxfordeconomics.com/resource/the-economic-impact-of-restricting-competition-in-5g-network-equipment/

- sectors that rely on highly specialised equipment or services as there may already be limited supply of alternative suppliers that have invested in the necessary research and development to provide alternative inputs; or,
- 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.

There is a further risk the requirements to obtain certification could slow down / deter innovation from both domestic and foreign businesses as this may be too time consuming for businesses to test and launch new products. At the extreme, businesses may choose to focus their investments on other locations where they consider their returns will be maximised and risks minimised.

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.[8] Taking into account the mix of inputs used by other sectors, the vendor screening measures would equate a **reduction in Portugal GDP of around €289 million**.[9]

Portugal spends around 1.61% of its GDP on R&D (lower than the average across the European Union of 2.3%).[10] An increase in the use of vendor screening measures could increase costs of ICT products and services and reduce volume Portuguese R&D investment. This is especially relevant for the ICT sector which has been growing quickly representing 10% of the Portuguese GDP.[11]

Impacts on trade and economic output

Discriminatory cybersecurity trade measures that rely on non-technical measures will reduce trade and economic output. The impacts on trade are summarised in Figure 2 below. The bars show the trade impacts in absolute terms. The shading of the bars shows the impact attributed to screening and compliance costs respectively. Overall, the usage of non-technical factors to screen vendors could lead to a **€169 million** reduction in extra-EU exports and **€37 million** reduction in intra-EU exports. There is also reduction in domestic output as the compliance

[8] See https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Reassessing-the-Productivity-Gains-from-Trade-Liberalization-43828

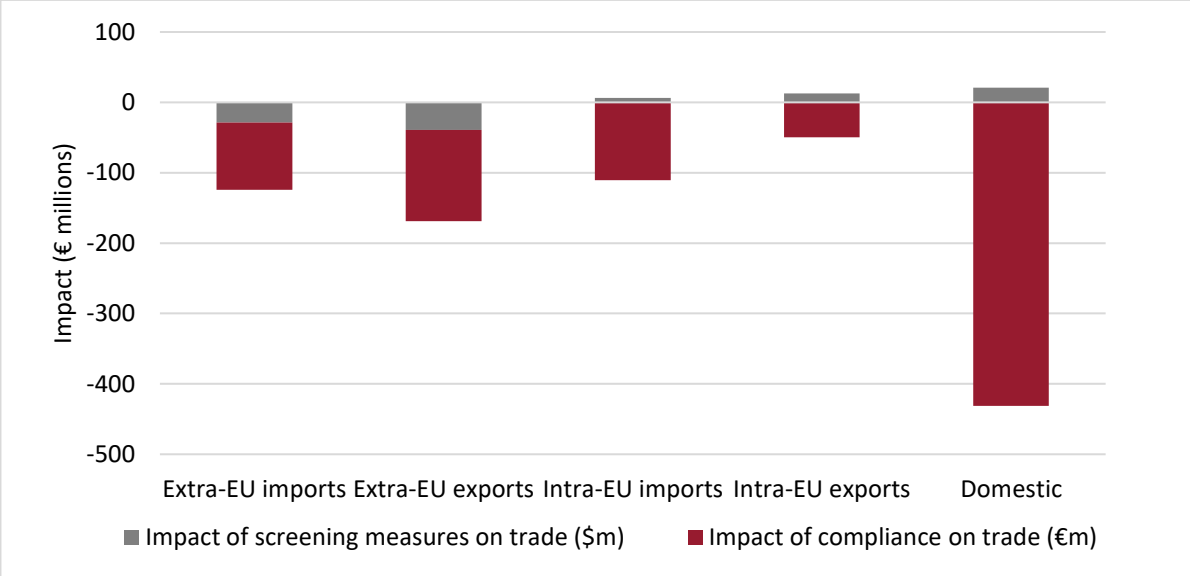
[9] Note that there is potential double counting between the effects of vendor screening on GDP estimated here and the trade-openness approach that was used in the next section, as both will include effects on ICT as an input into other sectors

[10] See https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=DE

[11] See https://www.trade.gov/country-commercial-guides/portugal-information-and-communications-technology

requirements impose pure costs on producers. As can be seen, the bulk of the impact is driven by incremental economic frictions associated with implementing the new regulations.

Figure 2 Distortionary impact on trade as a result of cybersecurity and discriminatory measures



Source: *Frontier Economics*

The impact on extra-EU export on trade comes via two channels:

- **€130 million** is due to the costs of compliance in implementing cybersecurity measures reducing the ability and willingness of firms to trade with the EU.
- A further **€39 million** is due to the discriminatory vendor screening measures which restrict the ability of firms to supply services, create uncertainty among suppliers and reduce transparency in regulatory decision making.[12] The effects of discriminatory measures reported here are likely to be highly conservative, as they are only estimated for direct effects on the telecoms and computer services sectors. However, these inputs are ubiquitous across the range of sectors, with ICT services representing around 1% - 2% of total output across these sectors. At a minimum we would expect the discriminatory measures to have a broad impact across a range of sectors, as the supply of these inputs becomes less competitive and more costly to procure. It may also reduce uptake and use of technology inputs, potentially resulting

[12] For practical reasons, the modelling is only able to analyse discriminatory measures in the "direct" sectoral sense – for example the impact of screening for telecoms and computer services on trade for the same sector. This is in contrast to "cross-sectoral" effects – for example the effect of screening ICT inputs on transport operators – as these effects are much broader than the direct effects analysed, but are much more complex to estimate empirically.

in adoption of less technology-intensive functional and business models, in extreme cases having more fundamental impacts in areas such as innovation or product offering. In turn, this will have impacts on the wider economy.

This implies that vendor screening measures would reduce the non-EU exports by €39 million which is equivalent to **5%** of Portugal's non-EU exports from the sector (non-EU exports of these sectors were €820.3 million).

The trade impacts will in turn affect GDP and productivity. Using relationships observed between openness to trade and productivity, GDP impacts can be estimated. Overall, for Portugal, the measures would **reduce GDP by around €289 million, of which €252 million is the impact due to the costs of implementing cybersecurity measures** and **€38 million is due to discriminatory cybersecurity trade measures (such as vendor screening)**, noting the latter estimate is conservative in its sector coverage.

Given that exports account for 23% of all the value added created in within the sector, vendor screening would have a non-trivial impact on the sector's value added. Overall (after accounting for offsetting impacts of increased domestic and intra-EU trade) vendor screening would contribute to a €38m loss in Portugal's GVA. This represents 3% of the value added created by the sector's exports.[13] It would be expected that a sudden decline in the sector's economic output would be associated with a fall in employment. If employment fell at the same level of the sectors' GVA then it would imply that vendor screening could put almost 1,000 jobs at risk.[14]

Conclusion

Enhanced cybersecurity measures are welcome but it is important for policy makers to ensure that the benefits of these measures outweigh the costs to consumers, businesses and the wider society. This means that the Portuguese Government should carefully manage this balance when implementing the NIS2 Directive into their country specific regulations.

In general, policy makers in Portugal have implemented cybersecurity policies that are proportionate and targeted at the technical nature of the risks (in line with the principles of the NIS2 Directive). However, there is a concern that some of the recently implemented cybersecurity policies could lead to policy makers relying on non-technical factors (e.g. geopolitical factors), which can lead to a negative net impact on consumers. Given this, policy makers in Portugal should focus on technical factors when assessing the degree of risk as this will ensure that any regulatory action is targeted and proportionate. This will also ensure that any action will achieve an appropriate balance between the benefits that can be achieved

[13] i.e. €38m / €1306m

[14] The Telecoms and IT sectors employ 137,000 people therefore the potential impact on employment could be approximated as: total sector employment 137,000 * impact on GVA (€39m)/ total sector GVA (€5,592m).

from enhanced cybersecurity measures against the cost of implementing these cybersecurity measures on end-users and businesses.