WWW.FRONTIER-ECONOMICS.COM

IMPLICATIONS OF NEW CYBER SECURITY MEASURES IN CZECHIA

28 JUNE 2023

Strong cybersecurity measures in Czechia 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 Czech Government and other Member States into their country specific cybersecurity laws and legislation (see Table 1).[1]

Cybersecurity measures, when designed appropriately, should enhance the strength and resilience of cybersecurity, 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 NIS2 measures for Czechia would lead to the following:

- an increase in costs for businesses of **€1.7 billion** to implement new regulations;
- a reduction in extra-EU exports of **€291 million** and extra-EU imports of **€200 million**; and
- a reduction in trade to the value of **€416 million**.

The NIS2 Directive provides a degree of discretion for policy makers to implement their country specific cybersecurity regulations. In implementing cybersecurity policies, there is a risk that Member States could impose obligations and restrictions which are stricter than those envisaged by the EU in its NIS2 Directive. This might be the case where Member States increase the scope of sectors to which regulations apply and/or apply stricter obligations than envisaged by NIS2. This risk is heightened if cybersecurity policy is unduly influenced by unrelated policy goals (e.g. if cybersecurity regulation is used to achieve geopolitical objectives or industrial policy goals rather than address the technical nature of the risks).

[1] See https://osveta.nukib.cz/course/view.php?id=145

One potential risk in Czechia's implementation of cybersecurity regulation relates to the proposed introduction of an "Ex-ante Mechanism" to restrict vendors, which goes beyond the scope of the NIS2 Directive. The Ex-ante Mechanism is designed to screen and prohibit suppliers from accessing the Czech market based on a range of non-technical factors (i.e. factors that are not directly related to the specific cybersecurity risk). The implementation of such vendor screening measures will likely lead to lower trade, reduced competition and slower innovation. The Czech Government should therefore carefully balance the need to introduce these screening measures against the potential costs on end-users and businesses.

There is also a risk that under-resourced cybersecurity authorities will resort to "easy to implement" policies (such as vendor screening bans based on non-technical criteria) which can impose significant costs on end-users. As such, the Czech Government should ensure that its cybersecurity authorities are sufficiently resourced to take on the additional responsibilities under the NIS2 Directive and address any concerns in a proportionate and targeted manner.

Czechia is in the process of implementing the NIS2 Directive but the proposed rules go beyond the intended scope of the Directive

Policy makers in Czechia are currently in the process of implementing the NIS2 Directive (see Table 1). However, the current proposals go much further than implied by the NIS2 Directive since it proposes to create an additional legislative instrument ("Ex-ante Mechanism") that extends the scope of cybersecurity regulations. The Ex-ante Mechanism is designed to allow the Czech Government to assess the trustworthiness of suppliers and intervene in the selection of suppliers for sectors with "strategic infrastructure" based on a range of non-technical factors (e.g. geopolitical factors).

There are a number of specific risks associated with this instrument. First, the sector scope of the Ex-ante Mechanism is extensive as it applies to a range of sectors such as internet service providers, electronic communication network operators,[2] cloud computing operators, electricity transmission system operators and railway infrastructure operators.[3] Second, the Ex-ante Mechanism deliberately uses "non-technical" criteria to assess the degree of risk (i.e. criteria which are not directly related to the cybersecurity risks, but instead relate to wider geopolitical characteristics). There is therefore a risk that if used improperly it could lead to substantial costs to end-users, businesses and the wider economy of Czechia which are explored below.

[2] Operators with over 100K active fixed connections or over 350K SIM cards.

[3] Also includes central government authorities, electricity generation providers (with installed power over 100 MW), electricity distribution grid operators, oil pipelines operators, fuel pipeline operators, gas transmission grid operators, gas distribution grid operators, air traffic control, air traffic navigational services and TLD domain names registrar operators.

Table 1 Indicative timeline for implementing the NIS2 Directive

Date	Process
Feb – Mar 2023	Official public consultation
May 2023	Submission to Government
May – Aug 2023	Government approval
Sep 2023 – Jun 2024	Parliament vote and approval
Jun 2024	President signature
Jul 2024	Entry into force

Source: NUKIB

NUKIB[4] has already relied on non-technical measures to screen and restrict vendors in other policies. For example, the Cybersecurity Act[5] currently requires businesses to take into account of "warnings" from NUKIB. These are issued by NUKIB to warn businesses about a risk of major disruption to the availability, integrity or confidentiality of their information and communication systems, thereby also creating a significant negative impact on the security of Czechia and its interests. However, NUKIB has been using these to warn businesses about the usage of certain foreign vendors based on non-technical factors that are not related to the actual nature of the cybersecurity risk. In other words, NUKIB considers that the "trustworthiness" of suppliers will be dependent on the legal and political environment in which the supplier operates.

Cybersecurity imposes direct costs on businesses affected

The cost of implementing the NIS2 Directive in Czechia is estimated to be **€1.7 billion** and this is equivalent to **0.52%** of the total business turnover across the affected sectors (for context the EC estimated that average ICT security spending as a percentage of turnover was 0.52% in 2020)[6]. 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. In 2020, there were approximately 1.04 million SMEs operating in Czechia, with the vast majority of these (1.01 million) being micro-sized enterprises that employed between zero and nine

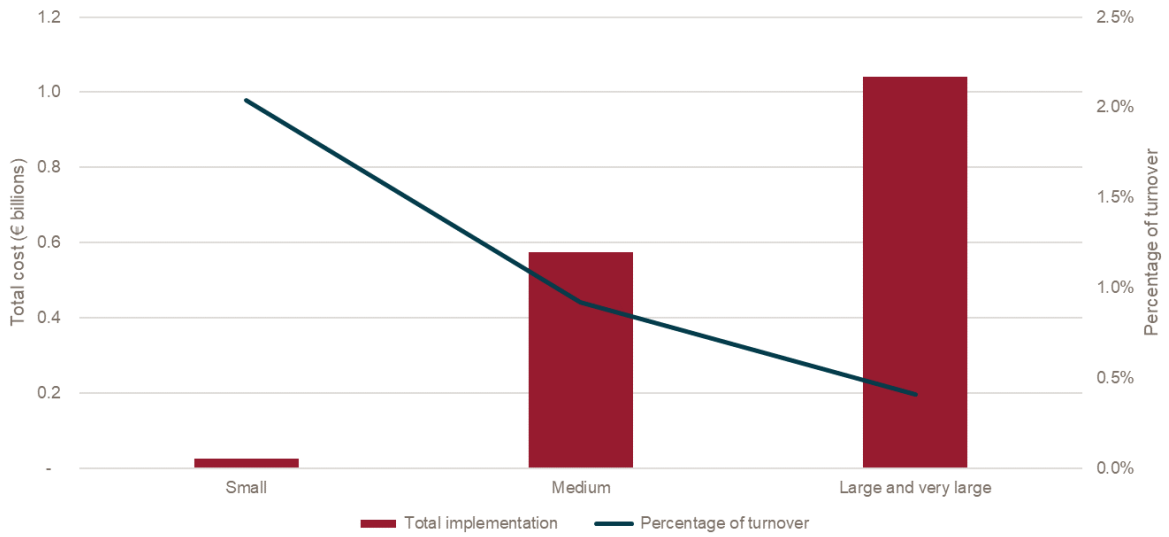
[4] The key national body overseeing the cybersecurity regulations in the Czech Republic is the National Cyber and Information Security Agency (NUKIB) established in 2017.

[5] The Cybersecurity Act imposes obligations on sectors which are dependent on electronic communication networks or information systems, where disruption may have a significant impact on the security of societal or economic activities. These include following sectors: energy, transport, banking, financial market infrastructures, health, water resource management, digital infrastructure and the chemical industry.

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

people. Additionally, there were around 31,600 small businesses, which had between 10 and 49 employees, and 6,579 medium-sized 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.

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.

Discriminatory cybersecurity trade measures to exclude vendors will impose substantial costs

Discriminatory policies which "screen" which firms can supply goods and services (i.e. trade with Czechia) will impose costs on businesses. Policy makers in Czechia are currently in the process of implementing the NIS2 Directive but NUKIB is creating an *additional* legislative instrument ("Ex-ante Mechanism") that extends the scope of cybersecurity regulations beyond those envisaged by the NIS2 Directive[7].

The Ex-ante Mechanism enables NUKIB to prohibit vendors from supplying businesses within Czechia where NUKIB considers that there is a strategic risk rather than a cybersecurity risk. The Ex-Ante Mechanism explicitly allows NUKIB to rely on *non-technical factors* (i.e. factors that are not directly related to the technical nature of cybersecurity) to determine the level of risk.

These policies will impose substantial costs on end-users, businesses and the wider economy. These costs are likely to be higher where they rely on non-technical criteria as they create uncertainty for businesses in how regulatory authorities will identify and assess risks; and they may not be proportionate to the risk (for example if they do not enable suppliers to adopt strategies to mitigate risks).

Discriminatory cybersecurity trade measures will increase costs of doing business within Czechia

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 now a risk that the investment costs will not be recouped, and that the project is no longer viable. Transactions costs may have a disproportionate impact where there are already transaction costs 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 under the Ex-ante Mechanism will likely create "economic frictions" that negatively affect trade, reduce competition and slow down innovation.

[7] See https://osveta.nukib.cz/course/view.php?id=145

Screening policies tend to have a negative net impact on consumers.[8] 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 Czechia as they may not consider it worthwhile to deal with the uncertainties and the processes of the Ex-ante Mechanism. This could subsequently reduce competition and increase prices for a range of sectors (that will be additional to costs highlighted above). These impacts can be felt in any sector where the need for specialised equipment means that there are limited supply of vendors, whether energy, medical devices or telecommunications equipment.

For example, a recent report highlighted that vendor bans on 5G equipment could reduce GDP by **€400 million by 2035**.[9]

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. Increased barriers to trade, like the Ex-Ante Mechanism, could deter or slow down innovation to the detriment of consumers and wider society. This is because the Ex-Ante Mechanism could reduce the investment from foreign vendors who are prohibited from supplying Czechia or they may no longer wish to do business in Czechia due to the uncertainties that the policy will generate. The Ex-ante Mechanism could further reduce investment from other local businesses due to higher input costs and lower competition.

This impact could be particularly harmful for those 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. This impact 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.

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.[10] Taking into account the mix of inputs used by other sectors, the

[8] 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.

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

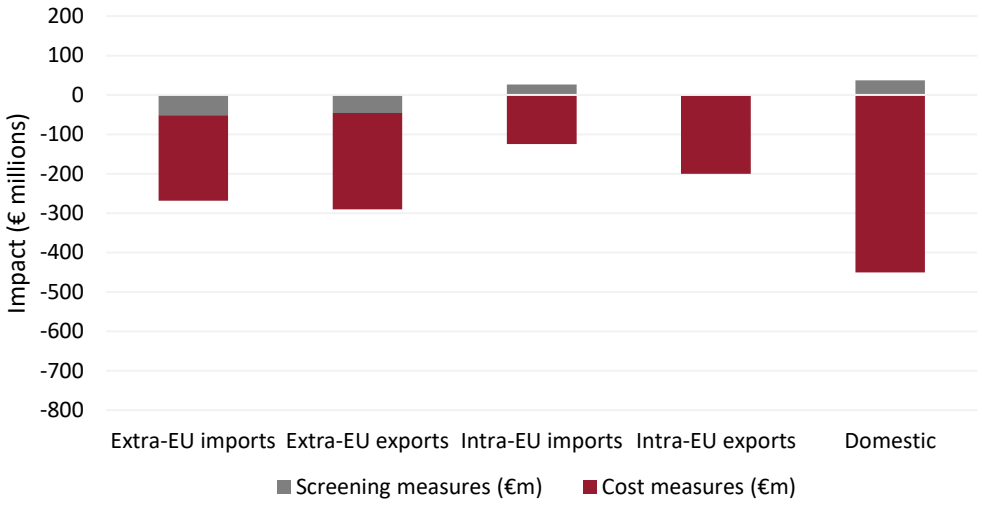
[10] See https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Reassessing-the-Productivity-Gains-from-Trade-Liberalization-43828

vendor screening measures would equate to an **increase in economy-wide tariff**, which would equate a **reduction in Czechia GDP of around €137 million**.[11]

Discriminatory cybersecurity trade measures will reduce trade and economic output

Discriminatory cybersecurity trade 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, while the marked line expresses these impacts as a percentage of total trade. The shading of the bars shows the impact attributed to screening and compliance costs respectively. Overall, the discriminatory cybersecurity trade measures could lead to a **€291 million** reduction in extra-EU exports and **€200 million** reduction in intra-EU exports. There is also reduction in domestic output as the compliance 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 Impact of cybersecurity policies on trade



Source: *Frontier Economics*

Note: *The cybersecurity and discriminatory measures are expressed as trade costs incurred when operating within the EU (for cybersecurity) or selling into that market (for screening). This is fed into a trade model to represent how trade flows adjust in response to these costs.*

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

- **€245 million** is due to the costs of implementing cybersecurity measures reducing the ability and willingness of firms to trade with the EU.

[11] 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.

- A further **€45 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 the discriminatory measures will likely 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 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.

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 Czechia the measures would reduce **trade by €416 million, of which €376 million is the impact due to the costs of implementing cybersecurity measures** and **€40 million is due to discriminatory cybersecurity trade measures (such as vendor screening)**, noting the latter estimate is conservative in its sector coverage.

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 Czech Government should carefully manage this balance when implementing the NIS2 Directive into their country specific regulations.

In general, the NIS2 Directive aims to implement a set of proportionate measures for the industry to manage risks based on the technical nature of the cyber-threats. Therefore, the Czech Government should adhere to the NIS2 Directive and avoid introducing non-technical measures that go beyond the NIS2 Directive as these will inevitably lead to disproportionate measures that impose higher costs for end-users, reduce willingness of foreign firms to invest in and supply Czechia, reduce competition and deter innovation. The Czech Government also needs to ensure that its cybersecurity authorities are properly resourced to administer these regulations based on the technical nature of the risk.

[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.