POSITION PAPER

PROPOSAL FOR A REVISED DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS 2 DIRECTIVE)

March 2022

Key points

- The NIS2 Directive review offers the opportunity to establish some missing links with other EU initiatives, in particular the Cybersecurity Act and the related cybersecurity certification schemes.
- While it is beneficial that small and micro enterprises (with exceptions) are excluded from the scope of the Directive, support is needed when they need to prove compliance, for example concerning supply chain risk assessments.
- Reporting thresholds and requirements should be kept proportional and realistic to ensure that the obligations are not overly burdensome and share relevant targeted information.
- The harmonisation of certification and standards use can help harmonise the European market and offers an opportunity to improve the uptake of agreed standards and certification schemes through support measures.

Background

With the adoption of the European Commission proposal for a revised Directive on the Security of Network and Information Systems (NIS2 Directive) on 16 December 2020, the European Commission aims at extending some aspects of the NIS Directive and at further harmonising its application throughout the EU, by providing clarifications, definitions and further explanation to the original version of the Directive.

SBS generally welcomes the clarifications and modifications that have been made to the Directive. As noted in our previous response to the open consultation, SBS is in favour of the efforts to strengthen the harmonisation of the Digital Single Market but remains wary of the negative impact that varying implementations between the Member States could have on the level playing field and spread of cyber-

Small Business Standards • Rue Jacques de Lalaing 4 • 1040 Brussels, Belgium
info@sbs-sme.eu • sbs-sme.eu • T +32 (0)285 07 27 • Transp. Register 653009713663-08

threats across borders. While SBS is in favour of a consistent approach across different Member States, the high level of detail in the Directive limits the ability of Member States to transpose the Directive into national legislation in the manner that best fits their situation, which may lead to disproportionately high administrative burdens for smaller companies.

Therefore, SBS is glad to see that the distinctions between requirements for "Essential Services" and "Digital Service Providers" have been removed, and further definitions have been provided for the identification of Operators of Essential Services (OES) and Digital Services Providers (DSP). **Most importantly, SBS is pleased to see that small and micro enterprises are explicitly excluded from this Directive**[1]. The burden of compliance with European legislation is often prohibitively high for most small companies, and therefore this exemption will allow them to continue to innovate and drive Europe's digital economy forwards.

However, these changes will bring a large number of companies under the remit of the Directive which under the old Directive may not have been originally assessed as critical at the Member State level. In principle expanding the scope of the Directive can be beneficial for European cybersecurity, however, this widened scope does not seem to consider the disproportionate requirements placed on companies that are not a vulnerability.

While it is likely that only a small number of the service providers excluded from the exemption (providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration) will be considered small or micro-enterprises, further clarification may be required. For instance, would a small or micro cloud service provider be excluded unless, for e.g. they provide a cloud service for a public administration? For this reason, it is still important to ensure that sufficient support measures are available for companies that do face compliance with the Directive – particularly for small and micro-enterprises.

Furthermore, the provision for companies to whom the Directive applies must ensure the security of their supply chains and service providers leaves the door open to small and micro enterprises being indirectly required to comply with the Directive. It is also likely that the security of supply chains will come with additional hidden costs for collecting and sharing the required information.

[1] However, the European Commission should acknowledge the critical role of some SMEs in European economies, for example where they handle critical data, especially along the supply chain. While the NIS2 Directive does include an obligation for national authorities to provide policy support for affected SMEs, this support must be sufficient to ensure that SMEs are able to meet the requirements without undue burdens. This support should also be made available to SMEs that are indirectly obliged to comply with the Directive, for example through compliance being required along supply chains as entities within the Directive's scope ensure their supply chain security.

The NIS2 Directive review offers the opportunity to establish some missing links with other EU initiatives, in particular the Cybersecurity Act and the related cybersecurity certification schemes

To increase the level of cybersecurity and to reach further harmonisation, there is a need to connect the NIS Directive with the Cybersecurity Act and related cybersecurity certification schemes. When the NIS Directive was first introduced, the Cybersecurity Act had not yet been implemented. This has led to different ways of implementation at national level. SBS is concerned to see that the Directive allows for Member State authorities to mandate the use of certification schemes for entities that fall under the scope of the Directive. While **certification schemes** ensure a high level of security, **they are often ill-suited to SMEs due to the cost of access and implementation** and can have a detrimental effect on business operations. If the schemes are based upon existing standards, these should be checked to ensure that their requirements and implementation do not place unnecessary burdens on SMEs.

This could be achieved through three means: the creation of a multistakeholder (including SMEs)process to recommend such schemes and standards; greater representation of SMEs in standardisation processes; and the implementation of an 'SME check' before schemes are approved to ensure that they are usable and accessible to all entities. A gradual approach would be recommended since SMEs cannot apply the same scheme of a multinational enterprise. Hence simplified schemes should be developed and adopted for SMEs.

Supply Chain Security and SMEs

While SBS advocates creating a level-playing field for small and micro-enterprises, which requires that they are not disproportionally affected by regulation and administration burdens, it is necessary to recognise the **importance of small and microenterprises for cybersecurity due to their role in supply chains**. This is especially important given the growing dependence on ICT systems and the internet in all sectors of the economy. In many sectors, small and micro-enterprises play a crucial role in supply chains and provide technologies, services, and products to other companies and often have access to their systems to provide their services.

Although the **NIS2 Directive explicitly excludes small and micro-enterprises from having to comply with the Directive**, the need for supply chain security and the requirement for entities to ensure that their supply chains and service providers are cyber secure (Article 18.3) could lead small and micro-enterprises to have to prove compliance with the Directive to retain business relationships.

The forthcoming risk assessment should ensure that security requirements for service providers and manufacturers in the supply remain proportionate and realistic relative to the level of threat and vulnerability. The Directive requires "increased diligence" during the procurement of Managed Security Service Providers and that data transformation and data analytics services take "all appropriate

cybersecurity measures". Defining appropriate cybersecurity measures can help ensure that the requirements of service providers remain proportionate.

For entities that fall under the scope of the Directive, the requirements outlined in Article 18.3 – which mandates that entities should ensure the quality and security of the products and services, as well as potential vulnerabilities, of each service provider and supplier – are likely to be heavily burdensome. At the same time, this would increase the likelihood of indirect compliance becoming the norm for companies within supply chains, as explained above.

While it is important not to overburden small and micro enterprises, if they are to be assessed for their security levels, being excluded from the scope of the Directive also means that they may be **excluded from any support measures that would lead to increasing their level of cybersecurity and to provide support (incentives, awareness, etc.) projects and funding (vouchers, etc)**. Therefore, while high thresholds and the exclusion of small and micro-enterprises are generally welcome, if the risk assessment shows vulnerabilities or that compliance with the Directive would be beneficial, **extending the coverage of the Directive may be beneficial to ensure that there are support measures in place, and that requirements for small and micro enterprises can be adapted to their specific circumstances**. To aid this, it would be important to have more information regarding both the requirements for entities affected by the Directive and how the risk assessment will inform cybersecurity requirements.

Reporting thresholds and requirements

While the promotion of standards ISO/IEC 30111[2] and ISO/IEC 29417[3] is a good step towards equal requirements across the Union, often accessing international standards is beyond the means of most small and micro-enterprises, as long as their implementation remains opaque.

Under Chapter IV, entities under the scope of the Directive are required to report any cybersecurity incident having a significant impact to the service they provide to the relevant CSIRT and competent authority within 24 hours. This time is quite short, and this will not always be possible.

While it is assumed that the exemption of small and micro-enterprises still applies to this requirement**, it should be further clarified how this requirement relates to service providers and supply chains, so that the reporting responsibilities for each type of entity are clear and information on how to do so is easily accessible.**

The requirement to report threats that "could have potentially resulted in a significant incident" (Article 20.2) places a large administrative burden on companies for threats that may never materialise into

[2] ISO/IEC 30111 Information technology — Security techniques — Vulnerability handling processes
[3] ISO/IEC 29147 Information technology — Security techniques — Vulnerability disclosure

security incidents. Furthermore, the requirement to notify customers of potential threats may undermine their response if an actual incident occurs, as well as jeopardising business relationships.

In general, SBS believes that the reporting of incidents should be encouraged as a means of levelling up European cybersecurity on a macro scale. However, the requirements for doing so, the thresholds for reporting and the means of reporting should be harmonised and easily accessible, so that the burden is neither prohibitive nor off-putting, for what is still a voluntary action. Moreover, before reporting an incident it is necessary to detect it. SMEs are often not in the position to effectively do so. They should be given access to support and help by ENISA, for example, or given incentives to invest in this topic with external support for competences.

SBS is glad to see that rather than suggesting that such standards are required for reporting by entities outside of the scope of the Directive, the Commission recommends the establishment of voluntary schemes by the Member States. Ensuring that these voluntary schemes are harmonised and not overly burdensome will be important for their uptake by small and micro enterprises and creating a level playing field.

As noted in Chapter V of the Directive, Member States are given the responsibility for allowing such voluntary reporting. It is key to ensure that the shared definitions of "significant incidents, cyber threats or 'near misses'" maintain reporting thresholds at reasonable levels. At the same time, leveraging existing European initiatives for reporting, such as the CSIRT network or the relevant national authority, is key to ensuring that companies can provide accurate and informative incident reports without being further burdened. The introduction of international standards, in this case, may be counterproductive if they are not already in common use by small and micro-enterprises.

Harmonisation of certification and standards use

To advance the harmonisation of the Digital Single Market and ease the burdens of compliance, the NIS2 Directive represents the opportunity to promote existing standards and certification schemes. Member States will "encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems." This may affect the procurement processes of companies, through cost increases both for suppliers and for the entities purchasing the service or product.

As mentioned above, international standards and certifications schemes can often be unsuitable for small and micro-enterprises, but the promotion of their use by national authorities has benefits for European cybersecurity and the Digital Single Market.

To encourage the uptake of relevant standards and certification schemes by small and micro-enterprises, the European Commission can follow the example of the SBS SME Guide on ISO/IEC 27001 to help small

and micro-enterprises implement security requirements for their needs. While the ISO/IEC 27001 has sufficient support for implementation, it is still complex and too costly for most small and micro enterprises to implement. An implementation guide such as the SBS Guide can be viewed as a "best practice" on how standards can be adopted by small and micro-enterprises.

Likewise, certification schemes can be harmonised across the European market to ensure a level playing field and mutual levels of security. The implementation of the Cybersecurity Act (Regulation (EU) 2019/881) and the establishment of the cybersecurity certification framework for ICT products, services and processes is an opportunity to develop certification schemes that can be easily accessed and applied by small and micro enterprises and are shared by multiple Member States.

Conclusion

The update of the NIS Directive is certainly necessary to ensure that Europe remains cyber secure, and introduces several needed actions, such as defining the types of entities that should be considered essential and providing an opportunity for the harmonisation of standards and certification schemes across multiple pieces of legislation. However, this does come at a risk of increasing administrative burdens and costs for SMEs. This is due, for example, to the supply chain risk assessment, which mandates companies to prove compliance to retain business relationships, without offering them guaranteed access to support (both financial and technical), due to their exemption from the legislation.

Further to this, the high thresholds and requirements for reporting foreseen in the Directive represent an opportunity to clarify and harmonise such actions across Europe, but currently run the risk of being overly burdensome, and thus less effective.

Small Business Standards (SBS) is the European association representing and supporting small and medium-sized companies (SMEs) in the standardisation process, both at European and international levels.

Co-financed by the European Commission and EFTA