Brussels, 02 October 2020

BSA's recommendations on the review of the Security of Network and Information Systems ("NIS") Directive (Directive (EU) 2016/1148)

BSA | The Software Alliance (BSA) welcomes the opportunity to provide input to the Commission's public consultation on the NIS Directive. BSA is the leading advocate for the global software industry. Our members are at the forefront of software-enabled innovation that is fueling global economic growth by helping enterprises in every sector of the economy operate more efficiently. In addition to our response to the consultation questionnaire, we would like to present the below recommendations to your attention.

Harmonisation

The threat landscape has increased considerably since the adoption of the NIS Directive in 2016, and the objectives of the Directive are more relevant than ever. Today cyber incidents rank among the most important business risk globally. Notwithstanding the achievements of the NIS Directive, the existing legal regime still carries shortcomings that impede the creation of a level playing field mechanism. While the NIS Directive has helped identify the relevant OESs across the Union, major disparities still exist as to the actual transposition, and therefore interpretation as to which sectors are part of the national lists of OESs. Consequently, several sectors which are not deemed to fall into the scope are included in the transposition of individual Member States, while in other cases entire sectors of Annex II are excluded. This constitutes a major challenge for OESs that operate across several Member States. Additionally, even if recognised as an OES in all these jurisdictions, the affected entity could nonetheless be required to comply with different regimes, i.e. both proactive and reactive designation models, different services falling within scope (and different service thresholds), varying levels of communication with the competent authorities, and in some cases, a lack of understanding of what is required as an OES which can stem from late transposition and a lack of available guidelines. Should the review include a legislative revision, the objective regarding OESs should focus on harmonizing the existing disparities, rather than on expanding the scope to new sectors. The latter would require extensive research and threat landscape analysis, supported by empirical data and evidence and input from the security community. Further harmonisation should be also considered for aspects like service definitions, thresholds, and reporting modalities, as well as for cases where an OES operates across several jurisdictions.

Scope

While the identification of individual operators as OESs should remain a national competence, the revision of regulated entities under Annex II and Annex III of the NIS Directive should be accompanied by legal provisions that ensure that Member States cannot opt-out or add entire (sub)sectors in the scope of their national legislation. This approach would help achieve a greater operational and organisational efficiency for the affected entities, and it would facilitate the handling

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

of cross-border incidents. Finally, special attention should be paid to the architectural specificities of some services or entities, which could face additional reporting complexity due to their dual OES and DSP role (for instance as they provide both Cloud and DNS or data infrastructure services). For such cases, overlaps and dual compliance and reporting regimes should be avoided.

Regarding the possibility to expand the scope to data centres (section 1.e.), we consider that this sector is already regulated by the NIS directive, through the inclusion of Cloud computing services into Annex III. Additionally, data centres that process data of OESs (i.e. while acting as a third-party technology provider to the latter) are also bound by the stricter requirements laid down under Article 14 and which also commit the third-party technology provider through its contractual obligations with its customer. Similarly, with regard to software products, the sector is also already covered within the Cloud services' inclusion in Annex III, notably through the Software As A Service (SaaS) principle. For the very limited cases where a software would not be delivered or serviced through the Cloud (i.e. when embedded in an industrial device which is not connected to the Internet), the incident reporting obligations would be irrelevant, as the manufacturer would not have the visibility of the incident affecting that specific software.

Differentiation between OES and DSP requirements

The provisions for operators of essential services (OESs) and digital service providers (DSPs) should remain risk proportionate and the differentiation between the requirements for each category should be upheld. This model has demonstrated its efficiency as it not only helps Member States to automatically triage their incident response when assisting affected organisations, it also helps OESs as their incident reporting is being handled in a priority fashion (note that this is also the case when the third-party technology provider assists its OES customer in its incident reporting). Additionally, contractual obligations between technology providers and their regulated customers often forbid the former to report incidents on behalf of the latter. Ultimately, this approach lowers reporting congestions and strengthens the overall resilience of the critical infrastructures. As an example, the COVID-19 outbreak has shown the importance of prioritizing sector-specific requirements.

Security requirements and applicable standards

While BSA welcomes the development of technical and operational guidelines by competent authorities, these should remain future-proof, technology neutral and adaptable to the specific context, purpose and environment. In this relation, highly prescriptive requirements risk limiting the ability of regulated entities to develop, deploy, service or use information security solutions (products, services and processes) that are best fit to their specific needs. Additionally, special attention should be paid to the necessity of developing requirements that are aligned with similar provisions in other EU Member States (and, from a market relevance perspective, internationally). This would allow for greater choice and flexibility, which will ultimately strengthen the overall resilience. Against this background, the concept of introducing mandatory certification is highly unsuitable both from a technological and operational standpoint.

Risk-based and outcomes-focused security requirements that are aligned across jurisdictions and interoperable across sectors help to improve security, enabling organizations to prioritize effectively, continuously improve, and coordinate with others. In this regard, we would recommend alignment with industry best practices and internationally recognized standards; for example with ISO/IEC 27013 or ISO/IEC 62443. Changes to requirements should be oriented around achieving a desired security outcome and reflect governance needs and resources; changing the requirements in a way that results in more incident notifications is unlikely to do so. Other examples include the 27000

family series, and ISO/IEC 27001 and 27002.

Finally, should the NIS review address cybersecurity aspects such as coordinated vulnerability disclosure, we encourage future provisions to align with international standards such as ISO/IEC 29147(2018) and ISO/IEC 30111(2019) that reflect globally adopted industry best practices in the field of coordinated vulnerability disclosure and handling.

Liability

In addition, liability exemptions or safe harbours for covered entitities who report incidents are critical and should be maintained in consistency with Articles 14(3) and 16(3) of the NIS Directive. Additional considerations include the necessity for competent authorities to provide clearer information to OESs and DSPs, including a one-stop-shop portal for information which can be useful when providers are cross-border in nature.

Information sharing and stakeholder input

As outlined above, greater alignment on reporting requirements of covered entities would be highly valuable and could significantly contribute to the robustness of the affected ecosystems. The NIS Cooperation Group and the CSIRT Network, supported by ENISA, could steer such processes as it has already set its cooperation structure. A stronger engagement with industry (OESs and DSPs) would ensure greater security. Competent authorities and CSIRTs should also facilitate the exchange of best practices/ information and policy expertise across sectors, countries and organizations, including government-to-industry sharing of cyber threat information and promoting voluntary industry efforts to share cyber threat information. By being more transparent with the cybersecurity community about incidents and how they were resolved, public authorities could increase market awareness and improve security capability. Learning from incidents should be a core objective of incident reporting obligations. In addition, the review is an opportinity to improve information sharing between and amongst CSIRTs. CSIRTs need to be able to consume more threat intelligence feeds, widening the visibility, providing greater insights to their stakeholder and making their intelligence more actionable.

* * *

For further information, please contact Thomas Boué at thomasb@bsa.org