ETNO POSITION PAPER

Revised Directive on Security of Network and Information Systems (NIS2)

Table of Contents

Introduction

ETNO welcomes the Cybersecurity Package proposed by the European Commission on 16th December 2020, which is an important part of the EU's digital transformation and recovery efforts. The package consists of **the EU Cybersecurity Strategy for the Digital Decade (Cybersecurity Strategy)**, a proposal for a Directive on the Resilience of Critical Entities, repealing the Critical Infrastructure Directive (EC) 2008/114, and notably, a proposal for a **Directive on measures for a high common level of cybersecurity across the Union ('NIS 2')**, repealing Directive (EU) 2016/1148 (NIS).

ETNO takes note of the NIS 2 proposal's aim to increase the resilience of public and private entities across the EU. However, we believe efforts to further streamline and clarify cybersecurity measures for all actors across the EU should be sought. Establishing the maximal common level of security should be one of the objectives of the proposal, which should better focus on **harmonising the cybersecurity regulatory framework** in the EU digital single market.

The coexistence of a range of European legislative acts and national security laws risks stifling legal certainty and consistency, possibly resulting in conflict of laws and even market distortion. This is especially true for companies operating in multiple EU markets. A notable example is provided by the interpretation and implementation of the 5G Toolbox, which differ significantly across Member States. Clarity on the interplay of cybersecurity measures in the NIS2, in the proposed Directive on Resilience of Critical Entities, and in the European Electronic Communications Code is also crucial.

While we do appreciate that the draft Directive puts increased emphasis on **supply chain risk management**, we believe that the proposed framework does not fully leverage the role of the supply chain itself in filling the gaps and strengthening the resilience of critical services. The growing role played by **providers of key technologies and services in the supply chain (notably hardware and software providers)** in determining the resilience of digital infrastructure needs to be reflected in a fairer allocation of responsibility for risk management.

Supply chains are becoming more global and complex, with a multitude of parties involved, and with an intricate web of roles and responsibilities. On its part, the telecommunication sector is undergoing an ever-increasing network sophistication, given the shifts to 5G and to a virtualised, software-defined and cloud-dependent infrastructure. This means that the networks and end-to-end services of tomorrow will be delivered by an ecosystem of operators, managed service providers and other business partners, where important functions and control points will move closer to the end-user and can be outsourced from telecom providers to other actors in the value chain.

Providers of key technologies and services are best placed to identify and solve the vulnerabilities in their products, services, or processes and thus to address cyber threats in the first place, before they spread across the whole supply chain. **Therefore, a key objective of NIS 2 should be to introduce direct risk management obligations upon key actors in the supply chain, especially hardware and software providers, since those closest to the problem are closest to the solution.**

In this paper, we highlight some specific points of concern and propose some areas of improvement.

Scope

The proposal expands the scope of the current NIS Directive by **adding new sectors**, notably including **Telecommunication Networks and Services, Data Centres and Trust Services** based on their criticality and by introducing a size cap. This means that all medium and large companies in chosen sectors will be included in its scope. It also leaves open the possibility of Member States identifying smaller entities with a high-security risk profile. **Clarification of certain definitions would be required, notably on 'Data Centres'** as this appears to be extremely wide reaching and it is not clear precisely which entities should be covered.

Whereas many hardware (equipment) providers are identified in Annex II of the NIS 2 proposal under 'manufacture – section C divisions 26 & 27 of NACE Rev.2'[1], to ensure the whole value chain is resilient and we avoid a fragmented security landscape, **providers of key technologies and services in the supply chain** should be included within the scope of the Directive.

These actors should be addressed as 'essential entities' and as such be subject to ex-ante supervision, by virtue of their delicate role in maintaining digital infrastructure and other critical services resilient. Otherwise, we would **miss an opportunity** to truly step up the level of cybersecurity in the EU as by leaving all these actors out of the scope of NIS 2, we miss vital parts of the security value chain. We need one integral framework for all actors.

Furthermore, the application of **recital 49** is extremely important for telecommunication network and service providers, which are currently dealing with the transposition and application of the European Electronic Communications Code (EECC) in various Member States, including its security measures under Articles 40 and 41. To ensure legal certainty and to minimise regulatory duplications, this provision should be moved to **an article** and its language strengthened. The European Commission should also assess whether additional EU-level guidance from ENISA is required to prevent inconsistencies and legal uncertainties for telecom network and service providers, should they be bound by national EECC transpositions applying to 40(1) and 40(2) and to separate measures under the NIS2.

Supply chain security

NIS 2 introduces new obligations for all essential and important entities on their **ICT supply chain and supplier relationships**. The proposed new supply chain risk assessment in Article 18 continues to place the burden and responsibility on the covered entities, namely essential entities and to a lower extent important entities. However, in today's digital world and tomorrow with the emergence of new technologies and multitudes of actors in the digital value chain, we need to ensure all these actors bear their share of the responsibility.

The proposal would require all entities to demonstrate how they have assessed the security level of the ICT products and services, and cybersecurity practices of their providers with particular attention

[1] NACE Rev.2 - Statistical classification of economic activities in the European Community (Eurostat, 2006) [Link]

to the security relationship between the entities and their data storage and processing providers, as well as network security services that have been outsourced to their parties. This will certainly create technical complexities. To ensure the best possible security across the ICT supply chain, these obligations should be **addressed directly to providers of key technologies and services in the supply chain,** who are best placed to analyse and mitigate their own security risks.

To address key supply chain risks and to assist the entities in managing cybersecurity risks related to the ICT supply chain, the Cooperation Group, the European Commission and ENISA would be tasked to carry out a coordinated risk assessment per sector of critical ICT services, systems or products including relevant threats and vulnerabilities, as per Article 19. Risk assessments would include both technical and non-technical factors. **Coordinated risk assessments are not in themselves sufficient to address the security and resilience of the value chain.** Again, the only way to substantially improve resilience and security of supply chains is the inclusion of providers of key technologies and services.

Risk management measures

According to Article 18(1), risk management measures must ensure a **risk-proportionate level of security** of network and information systems, taking into account "the state of the art". It is important to bear in mind that different actors operate equipment and systems with different lifespans, so the latest technology cannot be applied to all devices.

In general, the risk management measures enumerated in Article 18(2) are **far too detailed**, as not even the largest players would be able to undertake all the measures in all situations. The perimeter of application of all these measures needs to be streamlined and further clarified, to strictly reflect the elements for which the essential and important entities can realistically be responsible, not the whole system and its supply chain. All actors need to assume their own part of the responsibility in the supply chain. Legal uncertainty and unnecessary burdens on operators should be avoided.

Reporting obligations

We recognise the effort to try to streamline incident reporting obligations. Indeed, efforts to identify a single point of reporting in each member state would further streamline reporting in the context of the NIS2. The proposal however does reveal certain concerns.

Firstly, there is a need to better define and limit **what** needs to be notified. Entities should only need to report **significant** and tangible incidents and not 'potential' incidents. Significant cyber threats (based on the definition of Art. 2.8 of the Cybersecurity Act – linked to certification) should not be notified. NIS 2 should seek to incentivise an informal exchange of information regarding these significant cyber threats, while avoiding an excess of notifications that could result in administrative overload both for the notifying entities and the notified authorities, as well as in an erosion of trust in the services provided by the regulated entities. These unintended consequences would not be offset by any significant improvement in threat prevention.

Secondly, there is a need to better define **when** to notify incidents also. The current NIS 2 proposal states that, notification by the entities should take place "without undue delay and in any event within 24 hours after having become aware of the incident (…) which shall indicate whether the incident is presumably caused by unlawful or malicious action". The 24h initial notification delay is far too short for the affected entity to be able to establish the true root cause of incidents. Achieving established awareness of an incident in a large organisation may require standard procedures and due diligence. Therefore, this period should be longer, either by keeping the "undue delay" as foreseen in NIS 1, or perhaps if a delay has to be fixed, then aligned with the 72h notification period for data breaches under the GDPR. In addition, clarification is needed in reference to the latter part of the phrase 'after having become aware of the incident'. This should better read 'after becoming aware of the impact of the security incident' which would make the incident reporting more meaningful.

Thirdly, there is a need to better define **whom** should be notified. The Proposal states "the **competent authorities or the CSIRT**". This wording might cause legal uncertainty as it should only be one or another, not both bodies. This is in line with the issue of a single notification platform or SPOC. We would very much support a **centralisation or a single point of contact for incident reporting at national level**.

Certification

NIS2 empowers the Commission to adopt delegated acts establishing which categories of essential entities may be required to obtain a certificate and under which specific European cybersecurity certification schemes (Article 21). We believe that 'entities' should also include providers of key technologies and services in the supply chain (**hardware and software providers**), who may also be required to **certify their own products, services, or processes** as they are best placed to do so. Furthermore, it is important that certification schemes promote European industry and do not stand as a burden or barrier instead. Therefore, it would be necessary to introduce process optimisation mechanisms without lowering security levels.

Jurisdiction & Registration

According to Article 24, 'certain entities' (DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and CDN providers as well as certain digital providers) are under the jurisdiction of the Member State where they have their main establishment in the Union, which is typically where the headquarters of the entity are located, where the decisions on cybersecurity risk management are taken, or in the country where the company has the highest number of employees. ENISA will maintain a registry of these entities. The latter criterion related to employment does not respond to any security management rationale. The establishment that has **operational and managerial capabilities to implement cybersecurity measures** would be more suitable alternative to identify the main establishment.

Article 24 still fails to provide the necessary clarity for **cross-border services provided by pan-European groups**. It is not clear whether the main establishment refers to the headquarters of the legal entity concerned or to the headquarters of the group to which said entity belongs. If a group provides services in more than one Member State through subsidiaries that operate independently of the parent company as separate legal entities, these subsidiaries should fall under the separate and concurrent jurisdiction of their respective Member States.

Cooperation & Information sharing

Coordinating the management of cybersecurity incidents is essential, and its effectiveness depends on a practicable and smooth-running organisational structure. The possibility for Member States to designate one or more competent authorities responsible for the management of large-scale cyber security incidents and crises according to Article 7(1) could complicate the governance of such an endeavor. Requiring each Member State to designate **only one authority responsible** for operational management would simplify the setup of cross-border cooperation.

Regarding coordinated vulnerability disclosure, **we question the effectiveness of listing and giving access to vulnerability registries** as demanded in Article 6. It is important, especially in multi-party disclosure arrangements, to ensure confidentiality of information and to clarify who would have access to the registries and **what types of vulnerabilities**, be them technical or non-technical, should be included.

Article 26 is intended to enable the exchange of cybersecurity information. We very much support that Member States define, with the support of ENISA, specific **processes and technical specifications for the secure exchange of information**.

The existing channel of communication at national level between the national authority and the essential/important entities should remain the privileged reporting channel. Vulnerability reporting, if any, should remain at national level.

Administrative fines, supervisory and enforcement measures

Sanctions, as per Article 31, could reach a maximum of 10 million EUR or up to 2% of total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year (whichever is higher), for breach of the obligations laid down in Articles 18 and 20. Those Articles cover a **wide range of obligations of varying degrees of importance** to achieving the objectives of the Directive. The principle of **proportionality** in applying administrative fines is essential: sanctions should be intended as penalty for negligent conduct and their amount should reflect the impact of the breach. We note however that NIS 2 is proposed in the form of a **minimum harmonisation directive**, which could lead to further fragmentation across Member States when transposed. Establishing EU-wide thresholds for administrative fines as in Art. 31(4) should not be the objective of a legal instrument that, contrary to a regulation, does not aim for maximum harmonisation overall.

The proposed **enforcement measures** under Art 29(4)(h) and (i), which require entities to make aspects of non-compliance with obligations public, should be reconsidered on grounds of **proportionality**. Such measures could have a significant reputational impact on an entity that would extend even beyond the successful remedy of non-compliance and the due payment of the administrative fine.

In light of the broad scope of the proposed Directive, which will cover numerous small and mid-sized enterprises, it should be ensured that the cost of any security audit conducted by a third party as a supervisory measure remains reasonable and that the scope of the audit be proportionate to the size of the company.

Finally, in addition to the responsibility of companies for compliance with their obligations under the proposed Directive, Articles 29(5)(b) and 29(6) also introduce **responsibility and sanctions for persons** acting in the company. This exceeds the usual liability for organisational negligence and could result in personal liability at employee level and professional bans. We recommend removing these provisions. Article 17(1) already holds the management of regulated entities accountable for failure to comply with their risk management duties.

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this position paper, please contact Paolo Grassia (grassia@etno.eu), Director of Public Policy at ETNO.

European Telecommunications
Network Operators' Association

info@etno.eu
+32 (0)2 219 3242
WWW.ETNO.EU

@ETNOAssociation

Subscribe to our weekly digital newsletter