Position paper

ETNO Reflection Document on the EC Proposal for a Directive on Network and Information Security (NIS Directive)

July 2013

Executive Summary

- ETNO supports the European Commission's global approach to cyber-security and welcomes the proposed NIS Directive which recognizes the importance of security throughout the entire value chain.
- As eCommunication providers are already submitted to such obligations under the telecoms regulatory framework, we welcome their explicit exemption from the scope of the draft NIS Directive. However, we would welcome further clarification on the relationship between the various existing risk management and incident reporting frameworks (telecoms package, draft Regulation on e-identification). Indeed, the "exempted" market operators may also provide bundled services falling in scope of this proposed Directive. This calls for further legal certainty as to which measures apply to different services and more importantly to avoid unnecessary cumulative or inconsistent and burdensome obligations. Indeed, market providers should not be subject to different flavours of requirements depending on the service they provide.
- The European Commission [EC] should ensure that eventual further revisions of Framework Art. 13 remain consistent with the NIS Directive.
- ETNO believes that cross-sector regulation should replace sector-specific frameworks. In the long term, a cross-sector approach based on reasonable notification processes would benefit both business and customers and would avoid the need to keep aligned the obligations stemming from different Directives.
- The NIS Directive's end-to-end approach should be more explicit in establishing that non-EU based "market operators" are covered. Due to the global nature of the Internet, this is a key aspect with respect to customers' security and having a level playing field to allow all businesses to compete on an equal footing in the EU.

- ETNO welcomes the launch of the NIS platform as a way to consult all stakeholders of the global ICT value chain and exchange best practices. We welcome the DG Connect representative's statement that this Platform intends to guarantee a balanced cooperation between the public and private sector. ETNO would like to propose a NIS platform working group dedicated to the international enforcement of NIS obligations.

Introductory Remarks

ETNO welcomes the Commission's recent initiatives on Cybersecurity, in particular the European Cybersecurity Strategy and the accompanying Proposal for a Directive on Network and Information Security, as a major contribution to enhanced consumer trust and confidence in the digital era.

ETNO members take security very seriously. It is essential not only to protect their own networks and services but also that of their customers. Indeed, cybersecurity has both commercial and business value. We believe that any approach to cybersecurity must strike a balance between enhancing citizens' cybersecurity rights on the one hand whilst minimizing barriers to innovation for companies and providing the necessary flexibility for market operators to protect their networks and services. Indeed, there is no one-size-fits-all for risk management. Cybersecurity needs vary considerably depending on the sector (e.g. critical infrastructures, government etc.), the type of users (consumers vs enterprises), types of data etc.

A secure cyberspace is essential for a well-functioning Digital Single Market as Trust enables consumers to buy goods and services online and to take advantage of innovative services.

ETNO members have always been committed to high levels of security and resilience which are essential for the delivery of quality services. Security and secure networks and services are of the utmost importance. In today's globally connected world, Internet security is paramount, helps build consumer trust in services and so helps drive the growth of the digital economy. In most cases, security is considered as a quality differentiator and is at the core of the e-communications provider's business. Responsible operators devote a significant part of their budget to providing secure services and to promoting their ability to do so. Failure to lay such importance on security would lead to reputational damage, a loss of consumer confidence in services/providers and an increased liability risk. Security is also an element of differentiation as customers consider security key in their decision to choose one or another provider.

All the obligations and requirements established under the proposed NIS Directive must comply with the principles recognized by the Charter of Fundamental Rights of the European Union, notably, the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive must be implemented according to these rights and principles.

Specific Comments

Scope

Cybersecurity should be a shared responsibility amongst all actors: Administrations, private sector and consumers. Therefore, ETNO welcomes the proposed NIS Directive which recognises the importance of security throughout the entire value chain. ETNO supports the extension of security requirements to all Internet enablers as an essential element to create a level playing field and to ensure that all players offering services to EU citizens are subject to the same basic security requirements.

Currently, and based on art. 13a and art. 13b of the Framework Directive (Directive 2009/140/EC), only e-communications service providers are subject to obligations regarding minimum security requirements and the reporting of security incidents.

Against this background, we welcome the recognition that a number of market players are excluded from the scope because they already fall under existing obligations (e-communication providers and trust service providers). We feel that further clarification on the relationship between the various existing risk management and incident reporting frameworks (telecoms package, draft Regulation on e-identification) is needed. Indeed, the "exempted" market operators may also provide bundled services falling within the scope of this proposed Directive (eg cloud services). This calls for further legal certainty as to which measures apply to different services and more importantly to avoid unnecessary cumulative or inconsistent and burdensome obligations. Indeed, market providers should not be subjected to different flavours of requirements depending on the service they provide. This aspect also needs to be taken into consideration with regards to the designated "competent authority".

The e-communications services and network providers are increasingly competing with new players from outside the telecoms sector and often outside the EU. It is important that all actors of the value chain providing services of key societal and economic value be subject to the same obligations, namely, the requirements to adopt risk management practices and to report security breaches. Independently of their geographical location or their economic sector, all providers offering the same services shall be subject to the same requirements in order to achieve a true level playing field for all businesses to compete on equal footing in the EU and to guarantee a consistent consumer experience.

Software and hardware manufacturers, currently excluded from the scope of the Directive, should also be covered by the proposed Directive as this would help to create "a single market for cybersecurity products", one of the objectives of the Strategy, thus ensuring a higher level of security and resilience along the whole value chain. All telcos must comply with an operational and security validation procedure for equipment from external manufacturers. This validation must be based on tests and models stipulated by internationally recognized recommendations (for example, ISO 27000, among others) and on their own experience (regulatory and internal security policies resulting in operating procedures for the verification of appropriate security levels in the equipment).

However, given the limitations regarding the tests that telcos can carry out on any given equipment, it is impossible to discern whether such equipment:

- will fail in situations not covered by the tests (as it is not feasible from a technological point of view to generate a model of tests that verifies each and every one of the technical circumstances that may occur during the life span of a given product)

- contains any security vulnerabilities that will be discovered in the future

- will have a timely update or "security patch" to fix the vulnerabilities that are found

Telecoms operators have legal responsibilities. If any responsibility is breached for reasons outside the control of the telco, such as those expressed above in the limitations of equipment testing, ETNO companies shall be exempt from any liability, which shall then be directed to the manufacturer.

Currently the hardware and software manufacturer has no legal responsibility regarding security issues generated by their equipment. In other sectors (for example the automotive or aeronautics sector) the equipment manufacturer is responsible for severe failures that can occur with its components. Following this reasoning and given the fact that it is impossible for ETNO companies to conduct an overall security check of all components from third parties, and with evidence that the incidents were not caused due to negligence involving their operation, the responsibility for the incident shall lie with the manufacturer. The early detection and identification of potential threats are key for service providers to safeguard their customers.

Therefore, ETNO calls for the inclusion of hardware and software manufacturers within the scope of the Directive. This is justified by the importance of their role to reach the overall objective of the NIS Directive: create a culture of security and ensure a higher level of security and resilience along the whole value chain.

In this line, in its recent Opinion on Cybersecurity, the EDPS also questions why certain sectors that play an important role in network and information security have not been included in the scope of the Directive, such as manufacturers of hardware and software or providers of security software and services.

Harmonisation

Considering the global nature of the Internet, Network and Information Security challenges require a strong, coordinated European response without unnecessary regulatory burdens on e-communications service and network providers. Considering that cybersecurity is by definition cross-border, the proposal should aim to both further harmonise approaches within the EU and focus on a globally consistent approach, for instance referring to, but not being limited to, President Obama's Executive Order on Cybersecurity.

Within the EU and at international level, enhanced coordination and a common approach are needed to fight against illegal activities related to network and information security. Therefore, the European Commission should strive for better coordination (and effectiveness) at all levels in order to avoid overlaps with ongoing initiatives and to benefit from already agreed principles, and should seek closer cooperation with international partners around the globe.

Reporting

ETNO welcomes the risk-based approach followed in the proposed art. 14, which explicitly recognises that only incidents "*having a significant impact*" should be reported. This approach is necessary in order to avoid a counter-productive over-reporting. However, the notion of "significant impact" should be clearly defined in order to avoid an unharmonised interpretation which may lead to a lack of homogeneous approaches. It is important to note that the related thresholds cannot be defined according only to quantitative data but should be more appropriately take into account qualitative data. ETNO members are available to discuss this topic also at the NIS platform.

Indeed, notification requirements need to be flexible enough to avoid additional red tape and the downside of notification. More importantly, there is no one-size-fits-all approach for risk management. Cybersecurity needs vary considerably depending on the sector (e.g. critical infrastructures, government etc.), the type of users (consumers vs enterprises), types of data etc.

It is important to achieve the right balance between the costs incurred and the benefits derived. Reporting should not be an objective in itself but rather a way to enhance consumer trust in the online environment.

Competent Authority

Considering the extension of ,scope to Internet enablers and operators of critical infrastructure, the number of related competent authorities and the pan-European nature of incidents, the proposal should aim to have a one-stop shop/lead competent authority approach to ensure legal certainty for the notifying entities. Indeed they should benefit from having a single competent authority for reporting requirements and enforcement so that to avoid duplication of proceedings and duplication of possible sanctions. This is particularly important in the case of providers already subjected to such obligations (eg: e-communications providers) according to different rules, such as the e-privacy regulation. In this respect, as stated by the EDPS in its recent Opinion, the provision of this proposal should be carefully reassessed in order to guarantee consistency with the privacy regulation. . Moreover, it should also be the same authority in all the EU Member States which covers different sectors. To foster a harmonized approach, the EC could set qualitative security guidelines in order to let each local administration be responsible for assuring that these measures are implemented. A one-stop-shop reporting mechanism would avoid "over-reporting", which would be not only a burden for companies but also for the authorities themselves. Market operators should only report incidents once and not be subject to different or contradictory requirements. Reporting could be done to local administrations and from them, be shared with the public authorities that require different information exchanges. For achieving this, coordination between different public administrations must be improved.