Expert Contribution

ETNO Expert Contribution on the European Commission Consultation *"Improving Network and Information Security (NIS) in the EU".*

October 2012

Introduction

With a view to the forthcoming EU Strategy on Cyber-security, expected by end 2012, the Commission has launched this public consultation on "Improving Network and Information Security (NIS) in the EU" in order to gather input from interested stakeholders.

ETNO, the European Telecommunications Network Operators' Association, has 40 member companies who contribute actively to the achievement of the European Digital Agenda and who invest substantially in high speed broadband networks for the benefit of consumers. We welcome this opportunity to respond to the public consultation and we agree with the Commission on the need to enhance preparedness, strengthen the resilience of critical infrastructure and foster a cyber-security culture in the EU.

ETNO company members are key pan-European players in Networks and Information Systems and as such are strongly committed to ensuring a high level of security for all their networks and to supporting initiatives to improve security. Information and communication technologies form a relatively open ecosystem which is at the basis of the success of the Internet but at the same time, this renders the infrastructure and associated services vulnerable to attack.

Considering the international 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.

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. In order to achieve a level playing field across all sectors, ETNO believes that all actors in the supply chain providing services of key societal and economic value should be subject to the same obligations, namely, the requirements to adopt risk management practices and to report security breaches. In addition, all participants in the ICT value chain should benefit from incentive programs to undertake measures that enhance security.

Importance of Secure Networks & Services

Security and secure networks and services are of the utmost importance for ETNO companies. In today's globally connected world, Internet security is paramount, helps build consumer trust in services and so helps drive growth of the digital economy. In most cases, security is considered as a quality differentiation 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/the provider 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.

Shared Responsibility

ETNO believes that everyone plays a role in helping to ensure a minimum level of protection against cyber threats – Governments, business and consumers. The Commission is considering the introduction of a requirement to adopt risk management practices and to report security breaches affecting networks and information systems that are critical to the provision of key economic and societal services (e.g. finance, energy, transport and health) and to the functioning of the Internet (e.g. e-commerce, social networking). This would imply an extension of the obligations currently applicable to the electronic communications sector to other players.

Security is implemented across the full value chain of players and one weak link can destroy the whole system. Therefore, ETNO believes that there should be a level playing field established and that all actors in the value chain providing services of societal and economic value should be subject to the same obligations that are currently only applicable to the electronic communications sector.

The current EU legal framework for the e-communications sector (the recently reviewed Framework Directive 2009/140/EC and ePrivacy Directive 2009/136/EC) establishes new obligations regarding minimum security requirements and the reporting of security incidents as well as the notification of security breaches. Beyond these legal obligations, most ETNO members have implemented comprehensive security programs to minimize security threats. Therefore, ETNO believes that new regulation to enhance Network and Information Security is not needed for the sector. Additional regulation would imply additional costs and hamper innovation. Other players of the supply chain, however, should also be subject to the same minimum regulatory requirements in order to contribute to a global effort around enhancing Network and Information Security.

Harmonisation

The harmonisation of current regulation is important for ETNO members and particularly those that have a pan-European business. At international level, legal coordination and a common

approach are needed to fight against illegal activities related to network and information security. There are already various initiatives from different entities and therefore we should strive for better coordination at all levels rather than developing completely new structures which could imply overlaps and add complexity. Therefore, the European Commission should foster enhanced cooperation at the international level with other entities (eg: Council of Europe), in order to avoid overlaps with ongoing initiatives and benefit from already agreed principles.

Harmonisation is particularly important to address cross-border attacks and the coordination at national and European level of all stakeholders (public administrations, providers of e-communications services and networks and citizens) will help ensure that the major threats are identified. Therefore, the European Commission should foster enhanced cooperation at the international level with other entities (eg: Council of Europe), in order to avoid overlaps with ongoing initiatives and benefit from already agreed principles.

Awareness

There is a clear need for more awareness and an understanding of Network and Information Security issues, including the need to develop a “culture of security” in the European Union.

End-user education and awareness are key elements to ensure that all the players and organizations involved, including the end users of the services, are more prepared and thus can potentially reduce the impact of any security incident in any of those services.

Incentives

An effective overall approach to tackle the threat to cyber security would be to create significant incentive policies for all players in the ICT value chain. The European Commission has a role to play in promoting policies based on sound economic incentives based on cost risk analysis methods.