EDiMA
Shaping Internet Policy in the EU

EDiMA Position on the draft Network and Information Security Directive

Representing some of the largest Internet platforms operating at the European level and interested in the development of the European digital single market, EDiMA welcomes the European Commission's initiative to promote and strengthen Europe's security capabilities and to ensure a harmonised framework and approach to network and information security in Europe.

We applaud the aim of the Commission Strategy and the draft Directive proposal to achieve a coherent and coordinated approach to network and information security across the European Union (EU). EDiMA supports the objective of fostering a secure and trustworthy digital environment in the EU, as well as the increased and more efficient cooperation on cyber-security among EU Member States. However, to better ensure that the proposal achieves its stated aims, EDiMA believes that the Directive should:

- **cover only those services that are truly critical to the functioning of society and economy;**

- **be based on the principles of proportionality and grounded on a risk-based approach;**

- **needs to be consistent with reporting and security obligations already established in other European legislation (including the forthcoming General Data Protection Regulation);**

- **recognise existing international standards and best practices, and be consistent with emerging international cyber-security frameworks (such as the cyber-security framework being established as result of the President's Executive Order in the U.S.) in order to effectively counter rapidly evolving cyber-security threats that are global in nature;**

- **have a set of conditions to ensure the oversight, accountability, operations, transparency, and responsibilities given to the competent authorities', especially bearing in mind that the proposed Directive gives each Member State full flexibility to establish and designate a national competent authority on the security of network and information system as well as to avoid confusion and overlap with the role of Data Protection Authorities.**

I. Scope

The proposed Directive marks an important new step in creating an effective response to cyber-security threats, and should focus on truly critical aspects of the European economy. Taking a targeted and proportional approach will help to better use the limited resources of the competent national authorities in protecting those infrastructures whose failures would cause serious economic, health or security impacts. Casting a wide net to cover all enablers of information society services would not result in improved cyber-security, but rather would lead to the overburdening of national authorities by swamping truly critical incident reports in masses of non-critical ones. Furthermore, we do not agree that consumer IT

services and cloud computing service providers should be included as critical infrastructure organisations.

Within this approach, enablers of information society services should not be covered within the scope of the Directive. Subjecting a wide range of services such as e-commerce platforms, social networks, search engines, online review websites, online travel agencies, cloud computing providers or application stores to the same reporting requirements as transport or energy networks will not promote greater cyber-security in Europe. On the contrary, indiscriminately including all information society services would create unnecessary regulatory and administrative burdens for both reporting entities and national authorities. The vast number of information society services available in the internal market would swamp national authorities with non-critical incident reports thereby undermining their ability to effectively deal with critical services. This also risks creating a "compliance mentality" among market operators who will need to focus their financial and human resources on complying with disproportionately burdensome reporting requirements rather than being encouraged to continuously innovate their technology solutions to counter the rapidly evolving cyber-security threats. The Directive would end up applying mainly to operators that are irrelevant to the pursued policy objectives, thus hampering the cyber-security of infrastructures which are truly critical to European citizens and the economy.

It is not justified to treat the disrupting of online platforms services (such as search engines, online shopping, social media, online games, music services, online review websites, and online travel agencies) the same way as incidents that adversely affect the supply of electricity and gas across the Union, or the operation of airports, stock exchanges or hospitals.

A one-size fits all approach does not address the fundamental differences between critical infrastructure services and consumer services that provide a convenience or entertainment to the European citizens. A security incident or breach resulting in the temporary disruption of a transport or energy service will have a truly critical impact on the functioning of society, as opposed to the temporary unavailability of a search engine or an e-commerce website.

- Online platforms and services are a dynamic, innovative, and vibrant marketplace, defined by strong competition, consumer choice, and new services. The disruption of these services is unlikely to result in any substantial economic harm as consumers have the ability to use alternative services if one goes down.

- These services already fall under reporting and security obligations where personal data is concerned. A number of Member States have already introduced a breach notification in case of personal data losses, and the forthcoming European Data Protection Regulation will introduce security and notification requirements across Europe.

- A broad and legally undefined term such as "*cloud computing services*" could encompass virtually all online services irrespective of them being essential or vital, which could further undermine the effectiveness of the Directive by extending its scope to areas without any relation to critical information infrastructure protection;

- The non-exhaustive list of services that could possibly fall under the scope of the obligations creates long–term legal uncertainty and the potential for varying

national implementation, resulting in the further fragmentation of the Digital Single Market in the EU.

II. Critical Services

Defining Critical Services

Article 2 of the European Critical Infrastructure Directive (2008/114/EC) should serve as the basic criterion in defining critical infrastructure, namely *"(….) an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State".*

Obligations of Critical Services

For those services that meet the criteria of being a critical service, EDiMA believes that the Directive must be based on the principles of proportionality and grounded on a risk-based approach. Many of the services will have security and reporting obligations under other European Legislation, therefore the Directive needs to be consistent in order to avoid unnecessary double reporting, different thresholds, and security standards**.**

A. Harmonisation

The Directive should move towards maximum harmonisation to ensure a common approach across the EU. Minimum harmonisation, in particular regarding reporting and security requirements, could lead to the fragmentation of the internal market, legal uncertainty, and divergent obligations for operators that are active in numerous markets.

B. Notifications

In order to ensure that those market operators covered by the Directive are able to notify the competent authorities of security incidents in a timely matter, and that those authorities are able to efficiently collect and share information on risks and incidents, it is vital that they are able to directly notify the authority in which they are established.

In addition, it is important to realise that the benefits gained from sharing such information directly with law enforcement authorities are, in the majority of individual cases, not dependent upon making notifications public.

Article 14 of the Directive requires market operators to report to the competent security authorities incidents that have a 'significant impact' on the security of the core services it provides. The Article does not, however, specify the kind of information that would be valuable to report and share, which may well involve confidential and sensitive information.

In addition, the public reporting of a specific incident will usually alarm users without contributing to a solution. As public notifications proliferate, citizens may cease to take even the most necessary warnings seriously.

To this end, it is advisable to have a better drafting of Article 14, providing for a clearer and more precise definition of the circumstances under which the notice of security incidents

must be given. Public notifications of specific incidents should also be restricted to individual cases where:

- It is necessary to prevent or deal with an ongoing attack, or
- A company has refused to fix a serious structural issue. In this case, public reporting should be based on rigorous factual analysis which finds the company to be knowingly and/or consistently negligent.

Public reporting can, however, play an important role when it comes to aggregated information that compiles data about a large number of incidents. Aggregated information can provide insights into the predominant origin of threats and the ways in which attacks are adapting to defences.

Reporting on security breaches should also be aligned with the other reporting obligations, such as for breaches affecting personal data, in order to avoid an over-burdensome system that mandates different mechanisms for breaches that are often the same and to minimise the amount of data that should be collected, stored, and processed.

C. Audits

Ex post audits are an important means of holding market operators to their obligations. However, we are concerned with the notion of regularly auditing companies that have not proven to be irresponsible and unresponsive partners in dealing with cyber-security threats. Responsible internet intermediaries have a vested interest in combating cyber attacks, and dedicate significant resources to that end. The unpredictable nature of those attacks means that market operators must be on constant alert to deal with any eventuality. Any requirement to be prepared for regular audits adds to the significant burden of ensuring security, thereby creating substantial costs and potentially stretching resources and undermining defences. Moreover, this approach sets a precedent which could eventually lead to governments conducting drastic and aggressive audits against foreign companies. While this may be less of a concern within the EU, there is a significant risk that certain non-EU countries would adopt such a strategy, using the EU model as a justification. Thus, we believe that audits should only take place when a company has demonstrated consistent negligent behaviour.

D. Standards

Public sector actors can play a useful role in assessing standards and encouraging their development. However, given the continuously adaptive nature of cyber threats, and the imperative of internet companies to continuously adapt and innovate, obligations to conform to specific standards will hinder security and stifle economic growth, market access, and global trade. Recommended standards should be global, voluntary, and industry-led. Moreover, recommendations should be made on a 'results-oriented' basis, allowing companies to adopt measures of their choosing which are equivalent to those recommended by public sector authorities.