NIS Directive: Getting the Scope Right

Executive Summary

To avoid undermining its usefulness to meet its policy objective, the NIS Directive must remain limited to those infrastructures and services that are essential to the stable functioning of the internal market. To maximise its impact, it should seek to create a common harmonised European baseline of network and information security for these infrastructures and services.

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled €1.9 trillion in 2012 and directly supports more than 4.2 million jobs in Europe.

* * *

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts 53, B-1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: Roger Coelho; roger.coelho@amchameu.eu +32 (0)2 289 10 18

POSITION PAPER

14 October 2014

A key objective of the NIS Directive is to improve the cyber-resilience of the European internal market by helping to mitigate the cyber threats that may disrupt its Member States' economies. The cyber risk management and cyber incident reporting measures proposed in the Directive can help in achieving this objective. However, these measures will only work meaningfully if they protect the right assets: those through which if compromised a cyber incident could have a tangible disruptive effect on a Member State's economy, public health or safety. To make a real impact:

- The Directive must focus solely on those infrastructures and services which are truly essential to the functioning of a Member State's economy, public health or safety. Unless an infrastructure or service is truly indispensable, its disruption is unlikely to threaten the functioning of the internal market. ***In cases where the internal market is not threatened of disruption, European legislative intervention would be neither necessary, nor proportionate, nor justified by subsidiarity considerations.***

- Therefore, the Directive must in particular avoid including in its scope any services that are not indispensable in their own right to the stability and functioning of the economy. A service, even if it is used by millions of individuals or businesses, is only vital or essential if its unavailability is likely to cause harm that cannot be mitigated. For example, ***a search engine or social network facing downtime is inconvenient, but it couldn't possibly debilitate any Member State's economy. Similarly downtime of one energy or transport facility alone does not generally imply service interruptions, let alone a disruption of the internal market. Reasons for this are twofold – the outage is unlikely to cause such an impact and secondly there are alternatives in the marketplace that can be switched to.***

- Therefore it is important to make it explicit that an operator listed in Annex II should only be in scope if it also meets all the criteria for inclusion defined in article 3(8).

- The Directive must not extend to services below the level of indispensable infrastructures and services because doing so would distract the compliance efforts of market operators and dilute the enforcement efforts of authorities. Instead of identifying and handling the few truly critical risks, they both would be busy wasting their resources on the many lesser incidents. ***Really significant threats and events might well go unnoticed in the mass of incidents perfectly irrelevant to the stability of any Member State's economy.***

- The Directive must not put unnecessary requirements on the suppliers to essential infrastructures and services. The operators of these essential infrastructures and services need latitude and flexibility to manage and coordinate their suppliers and providers as best suited to their actual needs. They will demand contractually of their suppliers that they take every measure needed for them to comply with the Directive's requirements. Extending those same requirements directly to the suppliers as well would be perfectly impractical: ***The supplier might not even know the full context in which its product is being used. It can therefore not be expected to manage the risks that only its customer is able to measure.***

- Moreover, extending the legal obligations of operators of critical infrastructures to their suppliers would also be highly counterproductive and create conflicts for suppliers: Precisely

because of who their customers are, these suppliers are bound by very strict confidentiality requirements towards their customers. Bringing them directly in scope would subject them to incident reporting obligations and potentially force them to breach that confidentiality, especially in cases where they are supervised by another competent authority and/or in another Member State than their customer. ***The provider of an "underpinning" service to an essential infrastructure operator could be forced to report an incident affecting that infrastructure behind the back of its own operator.***

To avoid undermining its usefulness to meet its policy objective, the Directive must remain limited to those infrastructures and services that are essential to the stable functioning of the internal market. To maximise its impact, it should seek to create a common harmonised European baseline of network and information security for these infrastructures and services. The emergence of inconsistencies and discrepancies between the national transpositions must be avoided at all costs, whether in terms of the scope of market operators covered, or in terms of requirements imposed on them. This also means having due regard to existing cross-border operations when evaluating the essential nature and the operational resiliency of market operators, in particular where substitutable facilities are located across borders. If the downtime of a facility in one Member State can be palliated through a facility in another Member State, that should be taken into account before including an operator in scope. Efficiency gains, economies of scale and optimal allocation of resources across the internal market should be incentivised.

The European Parliament's first reading report regarding scope represents signifant improvements to the Commission proposal and should be carefully considered in the trilogue negotiations.