POSITION PAPER

BUSINESSEUROPE

4 September 2013

BUSINESSEUROPE COMMENTS ON THE COMMISSION'S PROPOSALS FOR A CYBERSECURITY STRATEGY AND ACCOMPANYING DIRECTIVE

KEY MESSAGES

1. A **secure cyberspace is essential** for a well-functioning single market, but **legislation should be proportional,** allow for **a risk-based approach** and foster **private sector innovation**.

2. **The scope and definitions** of the proposed directive **should be clear** and interaction with other rules seamless.

3. Requirements on companies ought to be implemented **voluntarily**, in a **partnership between public and private actors**.

WHAT DOES BUSINESSEUROPE AIM FOR?

- *Incident notification should follow the principle of risk based approach and focus on actual events. Incident notification needs appropriate incentives to work best. Voluntary approaches might prove to be more efficient than mandatory reporting.*
- *Self-certification and industry-led mechanisms for implementing security policies and requirements are preferable. International standards or comparable standards should be followed.*
- *The notion of "significant impact" should be clearly defined in order to avoid lack of harmonisation in the implementation at Member State level.*
- *Companies operating in several Members States should be required to report to only one authority to avoid creating additional burden.*
- *Developing capabilities in people, processes and tools leads to permanent results.*

KEY FACTS AND FIGURES

148 000	***Computers compromised every day***
250 billion dollars	***Estimated cost of a major critical information security breakdown***

BUSINESSEUROPE

POSITION PAPER

4 September 2013

BUSINESSEUROPE COMMENTS ON THE COMMISSION'S PROPOSALS FOR A CYBERSECURITY STRATEGY AND ACCOMPANYING DIRECTIVE

BUSINESSEUROPE supports the Commission's recent activity on cybersecurity, in particular the communication "An open, Safe and Secure Cyberspace" and the accompanying proposal for a directive aimed at ensuring a high common level of network and information security across the Union.

A secure cyberspace is essential for a well-functioning single market, growth and jobs. Trust enables consumers to buy goods and services online and take advantage of innovative services, boosting the digital single market. Likewise, companies rely on trusted and transparent regulations as well as procedures to be able to implement such requirements effectively. Trust on both sides and a clear comprehensive framework are essential for completing the European digital single market. Cyber-incidents need to be avoided and prevented as much as possible. As they cause service disruptions and require resources to be fixed, they mean huge economic losses for business.

Cybercrime, economic and industrial espionage are growing and threats are severe. According to the European Commission, around 148 000 computers are compromised daily, and the World Economic Forum estimates that there is a 10% likelihood of a major critical information security breakdown at a cost of 250 billion dollars.

The existing EU legal framework already imposes requirements for the protection of infrastructure and services on the telecommunications sector. BUSINESSEUROPE acknowledges the Commission's proposal to apply cybersecurity requirements to other sectors. Such requirements must not create unnecessary burdens for companies and proportionality must be respected. With the growth of e-services and data transfers over the Internet, cybersecurity concerns almost all companies in every sector of the economy. Attacks can target critical infrastructure or involve organizations' key assets, such as theft of intellectual property. The requirements ought to be implemented in a cooperative manner between state and private sector actors, due to their substantial impact on companies' daily business.

BUSINESSEUROPE a.i.s.b.l
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

BUSINESSEUROPE shares the Commission's overall view of the importance of raising awareness about cybersecurity and taking action. However, we would like to propose additional principles for the cybersecurity strategy and have some reservations about the draft directive, which contains provisions imposing mandatory obligations on a variety of market operators. The scope of the proposed directive should be proportionate to the most serious threats for network and information security. We consider that the scope of the draft directive is unclear and the lack of clarity in the definitions could result in disproportionate and unjustified amount of red tape compared to the risk, especially for small companies.

1. The need of right principles for cybersecurity

BUSINESSEUROPE supports increased cooperation between public and private actors to foster innovation, exchange information and disseminate best practices on cybersecurity. Cooperation between public and private sector should generally be led by the principle of self-regulation and based on voluntary, industry-led sharing of best practices supported by global standards. The EU could also boost innovation through additional research and development funds and similar incentives.

We support the principles included in the cybersecurity strategy: the respect of EU's core values and fundamental rights in the cyberspace, access for all to the Internet and shared responsibility to ensure security, recognising the importance of security throughout the entire value chain. In particular, we welcome the multi-stakeholder approach in governing the Internet and the acknowledgement that the private sector should continue to play a leading role in the construction and day-to-day management of the Internet as well as corporate data transfers and especially IT processes.

BUSINESSEUROPE proposes additional principles that reflect tested practices from the corporate sector:

- ***Risk-based approach***: Given the nature of human activity, security can never reach 100%, but risks can be managed in an appropriate manner. Big risks with potentially severe consequences warrant a corresponding response and should take priority over smaller risks when limited resources are allocated within an organisation. Companies must assess evolving threats over time and administrative burdens from legislation should be proportional to the risk. Hence, a specific definition of what should count as a relevant risk or incident is of great importance. Only based on a clear definition one can assess the right appropriate legislation adequately. For example, the current definition of "incidents" does not only include active events, such as a hacking of a data base,

but “any circumstance”, which could result in situations where any vulnerability, even a missing software update in an operating system, could trigger mandatory incident notifications as long as a company in the value chain falls under the scope of the directive and the incident has a significant impact on the security of the core service, no matter how insignificant the service or the actual risk may be. The Commission must also clarify what is to be understood as an “incident having a significant impact”. Based on this definition, the need for mandatory requirements can be evaluated in accordance with additional benefits, financial burdens for market operators and the notion of actual caused harm. Disproportionate legislation could force companies to focus on legal compliance rather than on actual security. Counter-productive over-reporting must be avoided, in the interest of reporting mechanism efficiency. Notification requirements should respect the necessary balance between additional financial burden and benefits for companies.

- ***Applying proportionality tests*** would help to define relevant actions for specific actors and, therefore, should be consistently part of the policy process at stake. This is particularly the case for SMEs, which could be seriously affected by disproportionate requirements related to their security management systems. SMEs (according to the definition of Recommendation 2003/361/EC) that are not operating or providing critical infrastructure functions should be excluded from the scope.

- ***Developing capabilities in people, processes and tools*** leads to permanent results. Additional capabilities are needed for national Computer Emergency Response Teams (CERTs) and Network and Information Security (NIS) institutions in order to prevent and detect cyber incidents, reduce vulnerability, provide adequate support when needed and manage an effective response. Companies are called upon, in return, to increase their cyber resilience efforts.

- ***Private sector drives innovation***, which is the ultimate means to achieve cyber resilience as presented in the cybersecurity strategy. All legislation should be measured against the yardstick of fostering private sector innovation, not stifling it. Any regulatory intervention to ‘fix’ the technology involved could hinder innovation in an area which is rapidly evolving.

- ***Actions must be based on data***, not assumptions. Existing data require action to improve cyber resilience, but more data should be collected and shared between stakeholders, including between public and private actors, via trusted and voluntary information-sharing platforms.

2. BUSINESSEUROPE specific messages

Scope

In defining the proposed scope, BUSINESSEUROPE considers however that the draft directive does not sufficiently take into account the level of risk involved and the nature of activity of market operators. Currently the scope is neither clearly defined nor scaled on the basis of the risk involved. Apart from considering the size of companies, affected companies should also be considered based on their business, services, products and the notion of harm in case of an incident.

Interaction with other rules

Even though data security and the protection of personal data have overlapping implications, they address different concerns. Furthermore, we ask for consideration and further clarification on how the directive would interact and relate to other provisions in proposed or existing legislation, such as data breach notification in the General Data Protection Regulation proposal, incident notification in the EU Telecoms Framework Directive and in the Directive on the protection and security of critical infrastructures.

On the long term, cross-sector legislation should replace sector specific frameworks. A cross-sector approach based on reasonable notification processes would benefit both business and consumers and would avoid the need to keep aligned obligations in different directives.

Mandatory incident notification (Article 14)

It is of outmost importance to maintain the principle of 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 lack of harmonisation in the implementation at Member State level.

There should be also clarity on the purpose(s) and the expected outcomes of the incident notification requirements and the resources/expertise/technology that would be made available to take up these tasks by authorities at national and EU level. Other approaches might prove to be more efficient than imposed mandatory reporting. For instance, a public private partnership, such as the Network and Information Security (NIS) Public-Private Platform with clear objectives might be a better way forward than imposing strict binding rules.

Mandatory incident notification needs appropriate incentives. It is extremely important to avoid creating a culture of “naming and shaming”, which is not the most effective incentive to achieve better insight and transparency in security incidents. In this perspective, BUSINESSEUROPE supports the current formulation in the proposal for directive, according to which authorities should “duly balance the interest of the public in being informed” with “reputational and commercial damages”. It would be useful to include that “before any public disclosure, the company should have the opportunity to present its case to the competent authority”. We also support the formulation that authorities “need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes”.

Companies operating in several Members States should be required to report to one authority only, to avoid creating additional burdens. In this perspective, the “one-stop-shop” approach proposed in the current General Data Protection Regulation should be adopted. Also, when appropriate, the security reporting in the cybersecurity directive should be synchronised with the data breach notifications under the General Data Protection Regulation, with a single notification that is shared between authorities. Equally, in case of a single incident that also results in a data breach, possible sanctions must not be imposed on companies twice.

Certification and auditing

BUSINESSEUROPE supports self-certification and industry-led mechanisms for implementing security policies and requirements. In this perspective, international standards or comparable standards should be followed.

As a general principle, self-compliance mechanisms or independent third-party verifications should be preferred to national authority-led audits, in order to limit red tape and increase effectiveness. Companies operating across Member States’ borders should never need to perform more than one internal audit to demonstrate compliance with the requirements of security standards.

Capability development

Capability development is needed on many levels: governments, businesses and individuals. Strengthening CERTs, ENISA and other key stakeholders can contribute to promoting best practices and awareness with proper resources and training.

Businesses should step-up resilience through training, processes and technology. Companies and public administrations should embrace a culture of

risk management. Consumer trust is crucial, and companies should ensure that customers' data and core assets are sufficiently protected at all times.

Quick capability development requires openness and transparency in sharing best practices, experiences and data. Public entities could pave the way and report to the public on the number, severity and source of attacks that target the Commission itself.

Delegated acts

Delegated acts could also be source of legal uncertainty. For instance, article 14.5 foresees delegated acts to define the circumstances in which an incident must be notified, undermining predictability and making compliance more difficult.

* * *