Council of the
European Union

**Brussels, 16 July 2015
(OR. en)**

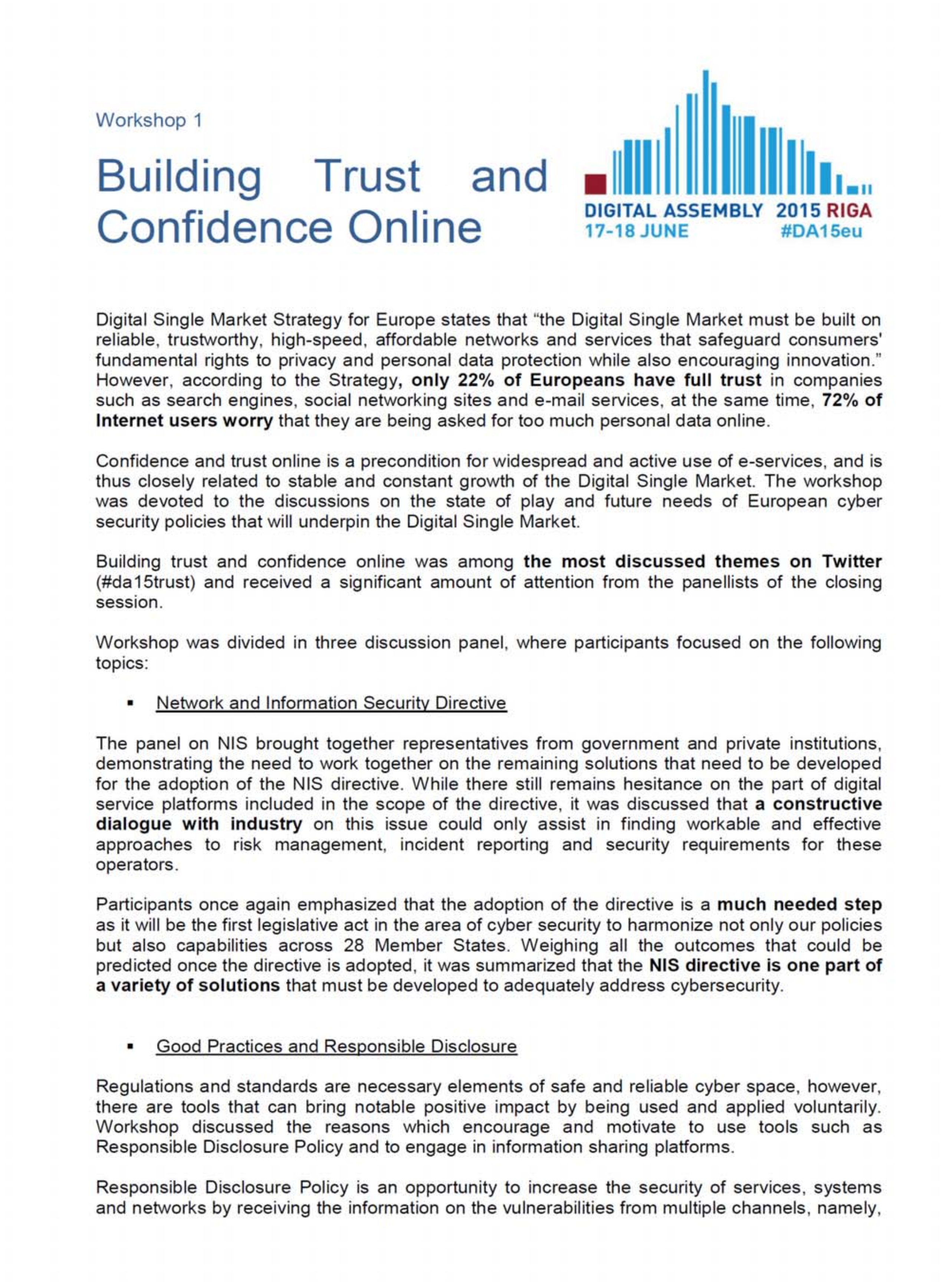
10975/15

CYBER 74

NOTE

From:	European Commission
To:	Delegations
Subject:	Building Trust and Confidence Online

Delegations will find in Annex the Report from Workshop 1 at the Digital Agenda Assembly on Building Trust and Confidence Online held in Riga on 17-18 June 2015.



Workshop 1

Building Trust and Confidence Online

DIGITAL ASSEMBLY 2015 RIGA
17-18 JUNE #DA15eu

Digital Single Market Strategy for Europe states that "the Digital Single Market must be built on reliable, trustworthy, high-speed, affordable networks and services that safeguard consumers' fundamental rights to privacy and personal data protection while also encouraging innovation." However, according to the Strategy**, only 22% of Europeans have full trust** in companies such as search engines, social networking sites and e-mail services, at the same time, **72% of Internet users worry** that they are being asked for too much personal data online.

Confidence and trust online is a precondition for widespread and active use of e-services, and is thus closely related to stable and constant growth of the Digital Single Market. The workshop was devoted to the discussions on the state of play and future needs of European cyber security policies that will underpin the Digital Single Market.

Building trust and confidence online was among **the most discussed themes on Twitter** (#da15trust) and received a significant amount of attention from the panellists of the closing session.

Workshop was divided in three discussion panel, where participants focused on the following topics:

- Network and Information Security Directive

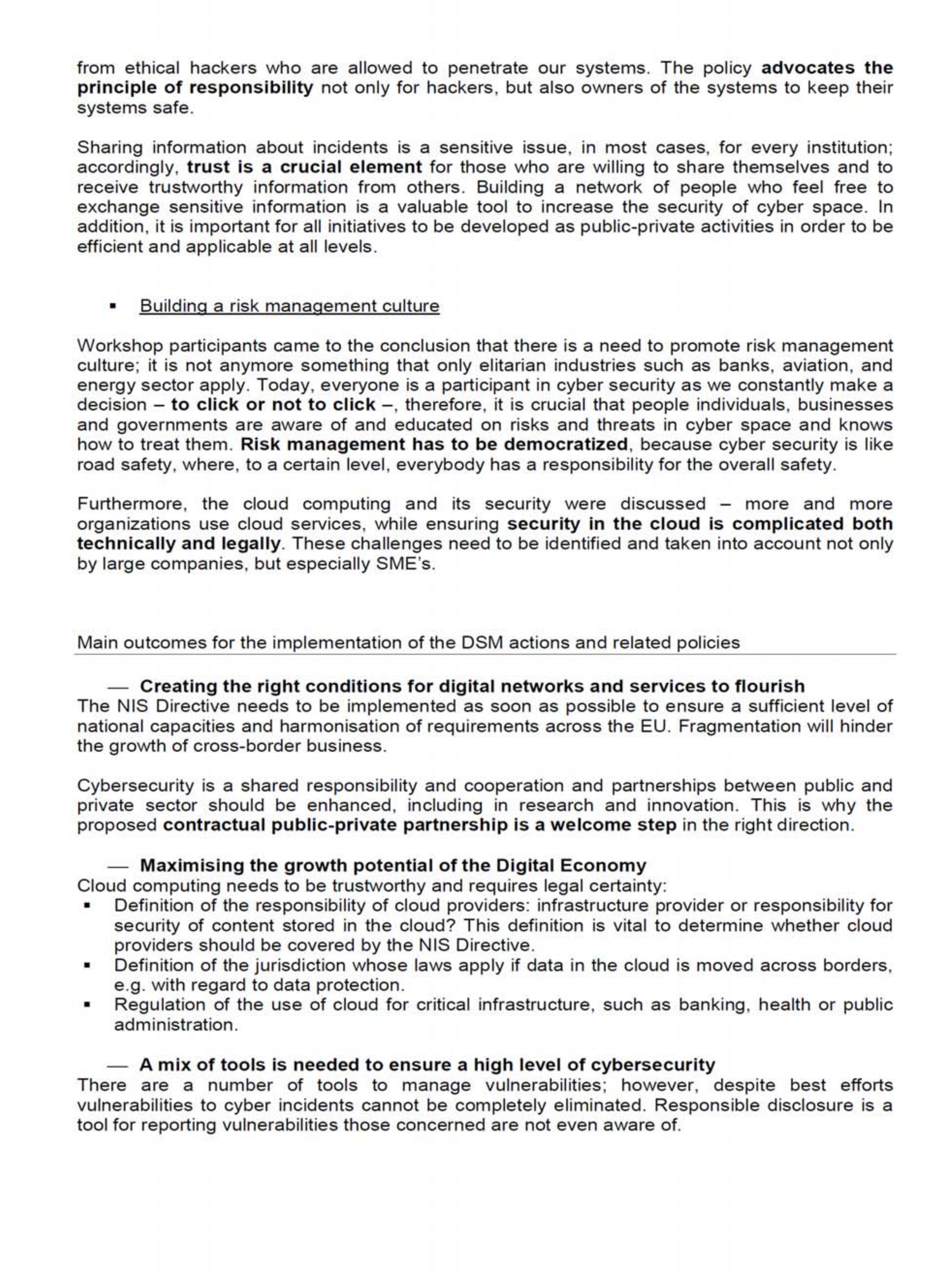
The panel on NIS brought together representatives from government and private institutions, demonstrating the need to work together on the remaining solutions that need to be developed for the adoption of the NIS directive. While there still remains hesitance on the part of digital service platforms included in the scope of the directive, it was discussed that **a constructive dialogue with industry** on this issue could only assist in finding workable and effective approaches to risk management, incident reporting and security requirements for these operators.

Participants once again emphasized that the adoption of the directive is a **much needed step** as it will be the first legislative act in the area of cyber security to harmonize not only our policies but also capabilities across 28 Member States. Weighing all the outcomes that could be predicted once the directive is adopted, it was summarized that the **NIS directive is one part of a variety of solutions** that must be developed to adequately address cybersecurity.

- Good Practices and Responsible Disclosure

Regulations and standards are necessary elements of safe and reliable cyber space, however, there are tools that can bring notable positive impact by being used and applied voluntarily. Workshop discussed the reasons which encourage and motivate to use tools such as Responsible Disclosure Policy and to engage in information sharing platforms.

Responsible Disclosure Policy is an opportunity to increase the security of services, systems and networks by receiving the information on the vulnerabilities from multiple channels, namely,



from ethical hackers who are allowed to penetrate our systems. The policy **advocates the principle of responsibility** not only for hackers, but also owners of the systems to keep their systems safe.

Sharing information about incidents is a sensitive issue, in most cases, for every institution; accordingly, **trust is a crucial element** for those who are willing to share themselves and to receive trustworthy information from others. Building a network of people who feel free to exchange sensitive information is a valuable tool to increase the security of cyber space. In addition, it is important for all initiatives to be developed as public-private activities in order to be efficient and applicable at all levels.

- Building a risk management culture

Workshop participants came to the conclusion that there is a need to promote risk management culture; it is not anymore something that only elitarian industries such as banks, aviation, and energy sector apply. Today, everyone is a participant in cyber security as we constantly make a decision – **to click or not to click** –, therefore, it is crucial that people individuals, businesses and governments are aware of and educated on risks and threats in cyber space and knows how to treat them. **Risk management has to be democratized**, because cyber security is like road safety, where, to a certain level, everybody has a responsibility for the overall safety.

Furthermore, the cloud computing and its security were discussed – more and more organizations use cloud services, while ensuring **security in the cloud is complicated both technically and legally**. These challenges need to be identified and taken into account not only by large companies, but especially SME's.

Main outcomes for the implementation of the DSM actions and related policies

— **Creating the right conditions for digital networks and services to flourish**

The NIS Directive needs to be implemented as soon as possible to ensure a sufficient level of national capacities and harmonisation of requirements across the EU. Fragmentation will hinder the growth of cross-border business.

Cybersecurity is a shared responsibility and cooperation and partnerships between public and private sector should be enhanced, including in research and innovation. This is why the proposed **contractual public-private partnership is a welcome step** in the right direction.

— **Maximising the growth potential of the Digital Economy**

Cloud computing needs to be trustworthy and requires legal certainty:

- Definition of the responsibility of cloud providers: infrastructure provider or responsibility for security of content stored in the cloud? This definition is vital to determine whether cloud providers should be covered by the NIS Directive.
- Definition of the jurisdiction whose laws apply if data in the cloud is moved across borders, e.g. with regard to data protection.
- Regulation of the use of cloud for critical infrastructure, such as banking, health or public administration.

— **A mix of tools is needed to ensure a high level of cybersecurity**

There are a number of tools to manage vulnerabilities; however, despite best efforts vulnerabilities to cyber incidents cannot be completely eliminated. Responsible disclosure is a tool for reporting vulnerabilities those concerned are not even aware of.