PUBLIC CONSULTATION ON NETWORK AND INFORMATION SECURITY (NIS) ACROSS THE EU

SUMMARY OF ANSWERS RECEIVED

This summary adds some further data on the categories of respondents and their views, in addition to the quantitative data which was published in Annex 1 to the Impact Assessment SWD (2013)32 accompanying the proposal for Directive on network and information security COM (2013)48.

1. Background

Network and information systems, and in particular the Internet, have become essential for our economies and societies. They facilitate the cross-border movement of goods, services and people and are hence crucial in the completion of the EU internal market. Public administrations, businesses and consumers all reap significant benefits from being online. Network and information systems also underpin complex systems in critical sectors such as finance, health, energy and transport.

Network and Information Security (NIS) incidents are, however, on the rise and when affecting critical information infrastructures could have serious consequences for the well-being of our citizens and societies. Problems caused by cyber incidents also erode public trust and confidence online. As many cyber incidents and attacks originate outside the EU, we are faced with a truly global challenge.

This is the background to the European Commission having announced, in its Work Programme 2012, an Internet security strategy. In order to come forward with a comprehensive strategy the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy decided to present a joint Strategy on cybersecurity.

One of the priorities for enhancing cybersecurity is to ensure the resilience of networks and information systems and a voluntary EU policy to that effect is in place since a decade[1]. To assess the various options for further improving the resilience and security of networks and information systems the European Commission conducted an impact assessment.

2. Options for improving NIS in the EU

The options assessed in the impact assessment, and reflected in the public consultation, included:

- Continuing with an approach based on voluntary cooperation and information exchange amongst Member States and between the public and private sector.

- A regulatory approach requiring the Member States to have minimum NIS capabilities in place, to cooperate and exchange information within a dedicated network; and requiring the private sector to adopt a risk management approach and to report significant incidents to competent national authorities.

- Recommending the taking up of a minimum level of capabilities at national level and a more structured cooperation and information exchange through a voluntary approach; and requiring the private sector to adopt a risk management approach and to report significant incidents through a regulatory approach.

[1] For an overview of the policy see Annex 2 to the Impact Assessment SWD (2013)32 accompanying the proposal for Directive on network and information security COM (2013)48.

The public consultation on network and information security, which ran from 23 July to 15 October 2012, contributed to the Commission's impact assessment, in particular regarding the envisaged risk management and reporting requirement. It also responded to a call from several Member States for further consultation on specific aspects of the Strategy.

3. Public consultation on NIS

a. Breakdown of replies by categories of respondents

The total number of respondents which submitted replies through the on-line tool was 169 and the breakdown of the related answers is reflected in the statistics provided below.

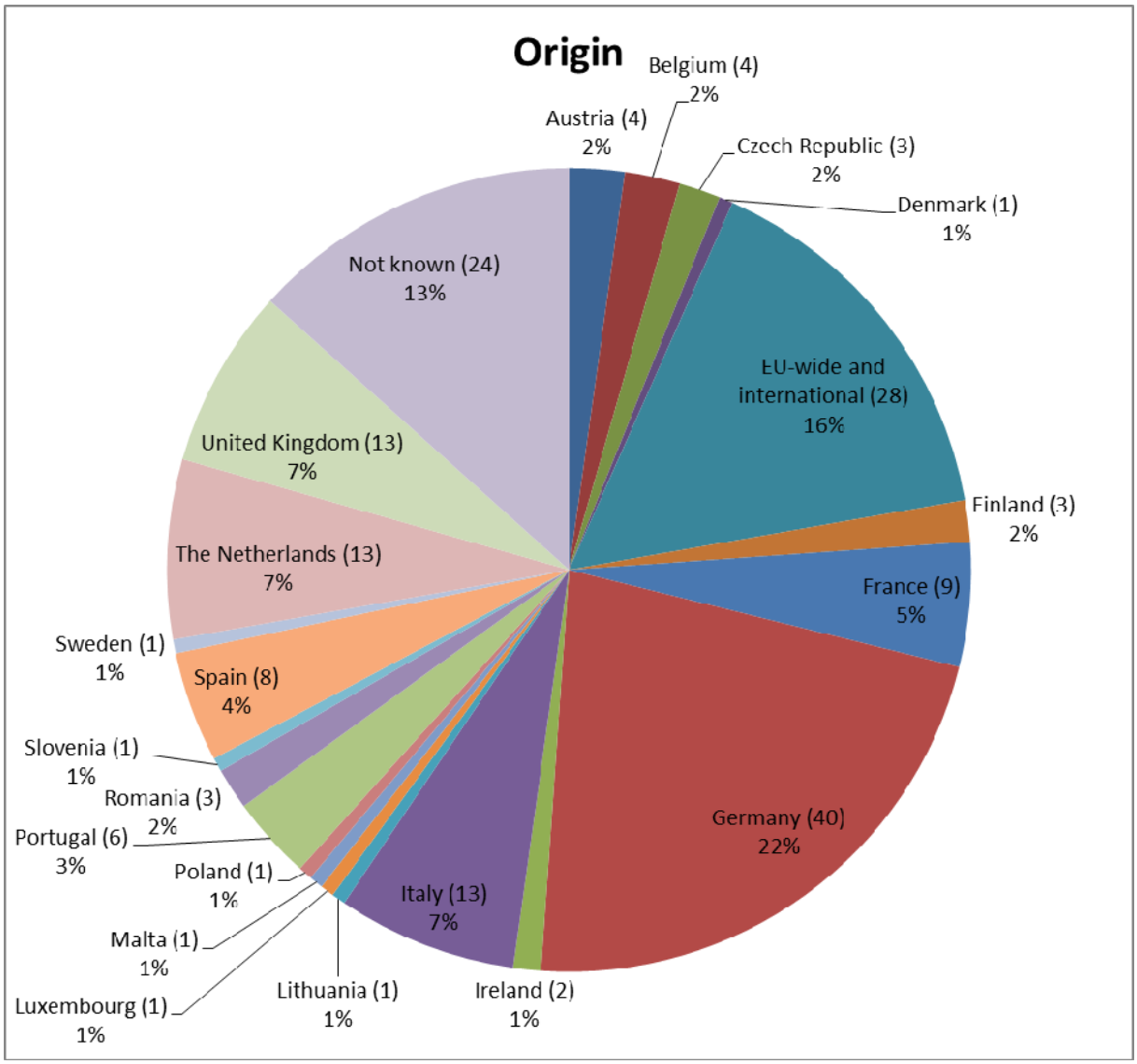
A further 11 organisations submitted written replies outside the on-line tool, bringing the total number of replies to the public consultation to 180; these 11 are not reflected in the statistics but their written contributions will be published online.

The total breakdown by type of respondent is the following: 88 individuals (of which 57 asked to remain anonymous); 12 public authorities (of which 5 asked to remain anonymous); 80 organisations or institutions such as businesses, research institutions and NGOs (of which 41 intend to remain anonymous). Some of the respondents indicated that they were replying in an individual capacity but at the same time representing an organisation. When publishing the replies (anonymised where necessary) the Commission chose to group those that were purely individual into one group and those that represented an organisation in another, to facilitate comparison of replies.

Type of respondent	Not anonymous	Anonymous	Outside the on-line tool (not included in statistics)	Total
Individuals	31	57	-	88
Public authorities	4	4	3	12
Other organisations	32	41	8	80 Businesses: 67 NGOs: 8 Academia: 5
Total anonymous/not anonymous	67	102	11	180
Total replies through on-line tool [66+103]	169		Total replies incl. outside on-line tool [169+11]	180

b. Origin of respondents

The geographical spread of the total 180 replies is represented below. It includes the origin of the anonymous respondents that are known to the Commission. The 'Not known' category includes the non-identifiable respondents of both not anonymous and anonymous respondents.



c. Main questions posed

The questions posed in the online public consultation focused on:

A. **Scale of the problem and evidence on impact**, to assess whether the respondents had experienced significant incidents and what are in their opinion the most frequent causes of NIS incidents.

B. **Improving NIS through an EU strategic approach**, to assess whether the respondents believe that there is sufficient awareness of threats and incidents in the

EU, that governments do enough in this field and what incentives can be set to ensure reporting of incidents and to raise user awareness.

C. **Improving NIS in the EU through risk management and reporting of incidents,** to assess whether the respondents conduct risk management; for which sectors of activity they believe it would be important to have NIS requirements; whether they would in principle agree with the introduction of regulatory requirements to manage NIS risks and what additional costs a requirement of this kind would entail for them. To assess also how effective information sharing could be achieved; to whom and at what level a requirement to report NIS incidents should be set; and what additional costs a reporting requirement would imply.

d. Summary content of replies

A. **Scale of the problem and evidence on impact**

Regarding the **Scale of the problem and evidence on impact** (56.8%) affirmed having experienced over the last year NIS incidents with a serious impact on their activities.

The respondents expressed the view that the most frequent cases of NIS incidents are third party/external failure (47.3%), malicious attacks (40.8%), human/technical errors (39.6%) and software/hardware failure (36.1%). Third party/external failure was the most frequently cited cause for individuals and NGOs. For businesses the most frequently cited causes were evenly divided between human/technical errors, malicious attacks and third party/external failure. For public authorities the most frequently cited cause was malicious attacks. For academia human/technical errors, malicious attacks and software/hardware failure were cited as causes for incidents. Environmental events/natural disasters was the least frequently cited cause (10.1%) for all categories of respondents.

B. **Improving NIS through an EU strategic approach**

Regarding **Improving NIS through an EU strategic approach a**ll categories of respondents (individuals, businesses, public authorities, NGOs and academia), in total 82.8%, expressed the view that consumers are in general not aware of existing NIS risks. A comparable high majority (82.8%) of the respondents also affirmed that governments in the EU should do more to ensure a high level of NIS.

When asked what kind of incentives would be needed to make companies and public administrations systematically report about NIS incidents, 57.4% mentioned support from NIS authorities to respond to incidents, 44.4% mentioned notification and report to NIS authorities, 44.4% mentioned publicity of incidents and establishment of performance ranking. Only 8.9% of the respondents affirmed that no incentives are needed in this regard.

Other incentives

Other incentives that were suggested by the respondents include: public performance ranking mechanism, though these also raise some concerns since agreed and meaningful ranking metrics are difficult to devise; public standard and certification (seal or logo that certified

companies can place on their websites) available that industries can choose to follow; government financing or tax incentives for cyber security improvements; reporting amnesties, liability safe harbours, compliance safeguards, or other rewards for due diligence; offering threat intelligence and mitigation advice in return for voluntary reporting (e.g. US Defence Industrial Base programme); certification against defined security standards; accreditation/assurance schemes to identify quality services; EU certified" online vulnerability check of citizens' computers; centres of excellence in the research domain and start-up clusters in EU, as well as of putting R&D in a global (end-to-end approach with a suitable governance, for instance in a public private cooperation like in an EIP); disclosure of (some) security breaches along with their financial consequences in private companies annual reports; security operations centres could be set-up as soon as an entity operates more than a defined level of resources (data centres, network points, etc.); development of a platform where private companies and public authorities can share technical data on ongoing incidents in near-real time; publication by manufacturers of security updates for devices, and auto-updates by devices so that security issues cannot be exploited; manufacturers should ensure that the default settings of the device are secure (e.g. residential broadband routers that often have default passwords such as 'admin' which are easy to abuse); continued support for software still in use is also crucial, currently there are broadly used operating systems that have vulnerabilities but are not supported by the vendor any more, hence all users of such software are vulnerable, often without even knowing it; companies to set up security pages; security breach reporting laws, as in the USA, not only to authority but also to the victims and the public, this has driven improvements in the USA, if you leak 50 million credit card numbers, and have to write to 50 million people at $10 each, that's enough to be an insurance claim – which drives the insurers to take an interest. Merely reporting to a regulator is unsatisfactory as regulators are often under-resourced, incompetent or simply captured.

Regarding the reporting of NIS incidents that may also constitute cybercrime to law enforcement, many respondents suggested that this objective could be achieved at EU level by establishing a legal requirement for NIS authorities, CERTs and affected users (39.6%) or only NIS authorities and CERTs (24.9%). On the other hand, 35.5% of the respondents, in particular businesses and NGOs, said that nobody should be legally required to report to law enforcement incidents that may constitute cybercrime, but that everybody should be strongly encouraged to do so.

All categories of respondents (individuals, businesses, public authorities, NGOs and academia) in total 84%, affirmed that businesses, governments and consumers in the EU are not sufficiently aware of the behaviour to be adopted to minimise the impact of the NIS risks they face. The respondents suggest that the best ways to achieve this objective would be in particular to give guidance at EU level to enable consumers to differentiate good security products and services (30.2%), to define compulsory security standards for goods and services at EU level (30.2%) or to stimulate the development of industry-led standards (18.3%).

C. **Improving NIS in the EU through risk management and reporting of incidents**

Regarding **Improving NIS in the EU through risk management and reporting of incidents**, 31% of the respondents affirmed that they do not have a process for managing risks in place and 54.2% of the respondents said that they do not have a budget dedicated to NIS. 30% of the respondents also affirmed that they did not have sufficient resources in place to counter and minimise the effects of NIS incidents that have affected them.

The large majority of respondents expressed the view that the adoption of NIS requirements would be important or very important in specific sectors in particular banking and finance (91.1%), energy

(89.4%), transport (81.7%), health (89.4%), Internet services (89.1%) and public administrations (87.5%).

A large majority of individuals and NGOs and half of businesses and academia (in total 66.3%) would also in principle be favorable to the introduction of a regulatory requirement to manage NIS risks, of those respondents 84.8% would prefer that such as requirement is set at EU rather than national level; 70.5% of those respondents also suggested that this requirements should entail a general obligation to adopt state of the art measures proportionate to the risks identified rather than prescribing specific actions.

Some of those respondents indicated that those who should be subject to these requirements are all business and consumers providing or using network and information systems (41.5%) whereas others (41.5%) said that only business providing or using network and information systems underpinning vital services for society (i.e. transport, energy, finance, health, Internet services of general interest, water) should be subject to this requirement.

The respondents stressed that a requirement to adopt NIS risk management according to the state of the art would entail for them no additional significant costs (43.6%) or no additional costs at all (19.8%). 36.5% of the respondents said that this would entail significant additional costs for them.

Regarding the question on what would constitute an incentive for effective information sharing on threats and incidents 37.9% preferred to establish a requirement to report significant NIS breaches to the national competent authority, whereas 37.3% preferred to establish stronger public-private cooperation mechanisms. Individuals were equally divided between the two options, whereas businesses slightly favoured public-private cooperation and academia reporting to the national competent authorities.

The majority of the respondents (65%) expressed the view that if a requirement to report NIS security breaches to the national competent authority were introduced it should be set at EU level and affirmed that also public administrations should be subject to it (93.5%).

If this requirement were to be introduced at EU level, respondents mainly suggested that this should apply only to business providing or using network and information systems underpinning services which are vital for the functioning of the society (43.8%) or to all business and consumers providing or using network and information systems (34.9%).

The majority of the respondents (52.5%) also affirmed that a requirement to report security breaches would not cause significant additional costs for them and 19.8% said that it would not cause additional costs at all for them.

May 2013
CNECT/H.4 Trust & Security