COUNCIL OF THE EUROPEAN UNION

Brussels, 12 February 2013

6342/13
ADD 2

Interinstitutional File:
2013/0027 (COD)

TELECOM	**24**
DATAPROTECT	**14**
CYBER	**2**
MI	**104**
CODEC	**313**

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	7 February 2013
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	SWD(2013) 32 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT *Accompanying the document* Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union

Delegations will find attached Commission document SWD(2013) 32 final.

Encl.: SWD(2013) 32 final

EUROPEAN
COMMISSION

Strasbourg, 7.2.2013
SWD(2013) 32 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

Concerning measures to ensure a high level of network and information security across the Union

{COM(2013) 48 final}
{SWD(2013) 31 final}

TABLE OF CONTENTS

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

Concerning measures to ensure a high level of network and information security across the Union

1. SCOPE

This impact assessment covers policy options to improve the security of the Internet and other networks and information systems underpinning services which support the functioning of our society (e.g. public administrations, finance and banking, energy, transport, health and certain Internet services enabling key economic and societal processes, such as e-commerce platforms and social networks). This issue is referred to as Network and Information Security (NIS).

Under Article 4(c) of Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (ENISA): "network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

This impact assessment does not cover Member States activities concerning national security and defense.

2. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

2.1. Identification

Lead DG: Communications Networks, Content and Technology (CONNECT) Directorate General, former Information Society and Media (INFSO) Directorate-General.

Agenda planning: 2012/CNECT/003

2.2. Organisation and timing

The different aspects of the initiative have been discussed with a wide range of stakeholders. We have adopted an inclusive approach and respected the principles of participation, openness, accountability, effectiveness and coherence. The consultation included:

- Member States representatives responsible for enhancing the level of NIS and/or Critical Information Infrastructure Protection (CIIP). Discussions took place in the context of the European Forum for the Member States (EFMS) as well as in the form of dedicated meetings organised at the request of individual Member States. DG CONNECT received written inputs from 7 Member States.

A stocktaking exercise on the state of play of existing NIS capabilities and mechanisms in the Member States was carried out by Commission Vice-President (VP) Neelie Kroes via a letter sent to relevant Ministers in the Member States on 28 November 2011. Almost all the Member States took part in this exercise. A follow-up letter was sent by

VP Kroes to the relevant Ministers following the Telecom, Energy and Transport Council of 8 June 2012.

Five Member States prepared a non-paper prior to the EU Conference on Cyber-Security that took place in Brussels on 6 July 2012 and that was jointly organised by the European Commission and the European External Action Service.

- **Private sector** representatives, including:

– Individual electronic communications service and network providers, Internet service providers, and industry associations (e.g. ETNO, EuroISPA, EuroIX, etc.);

– suppliers of hardware and software components for electronic communications networks and services, and industry associations (e.g. DigitalEurope, which represents large companies and SMEs);

– providers of products and services for Network and Information Security;

– representatives from the banking and financial sector and from the energy sector

Discussions with the private sector took place in the frame of the European Public-Private Partnership for Resilience (EP3R)[1], in the Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids[2] as well as in bilateral meetings. A number of relevant private sector players sent written contributions to the Commission.

- The **European Parliament**, in particular in the **Industry, Research and Energy (ITRE)** and **Security and Defence (SEDE) Committees**.

- The **European Network and Information Security Agency (ENISA)** and the Computer Emergency Response Team (CERT) for the EU institutions (**CERT-EU**).

- An online **public consultation**[3] feeding directly into this impact assessment was open on the European Commission website from July 23 to October 15 2012[4]. A total of 169 responses were received via the online tool. A further 10 responses were received in writing by the Commission, bringing the total number of replies to the public consultation to 179. The public consultation focused on a) the scale of the problem and evidence of its impact b) options for improving NIS though an EU strategic approach c) options for improving NIS through risk management and reporting of

1 The European Public Private Partnership for Resilience (EP3R) aims to foster the cooperation across Europe between the public and the private sector to develop coordinated strategic policy objectives as well as tactical/operational measures to strengthen security and resilience in CIIP

2 http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm

3 http://ec.europa.eu/information_society/digital-agenda/actions/infosec-consultation/index_en.htm

4 http://ec.europa.eu/information_society/digital-agenda/actions/infosec-consultation/index_en.htm

incidents. A summary of the questions addressed and the answers received to the public consultation is provided in Annex 1.

The total breakdown by type of respondent is the following: 88 individuals (of which 57 intend to remain anonymous); 11 public authorities (of which 5 intend to remain anonymous); 80 organisations or institutions such as businesses, research institutions and NGOs (of which 41 intend to remain anonymous). Amongst the companies that responded:

– 46% were large companies

– 20% were Small and Medium Enterprises (SMEs)

– 34% were micro enterprises

- A discussion with the **general public** was organised in the context of the 2012 Digital Agenda Assembly[5].

An impact assessment Inter-Service Steering Group was set up. The following Commission services participated in the group: SG, SJ, DG AGRI, DG COMM, DG ESTAT, JRC, DG CLIMA, DG COMP, DG ECFIN, DG EAC, DG EMPL, DG MOVE DG ENER, DG ENTR, DG ENV, DG SANCO, DG MARKT, DG HOME, DG JUST, DG REGIO, DG RTD, DG TAXUD, DG TRADE, DG BUDG, DG DIGIT, DG HR. The EEAS also participated in the group.

The Inter-Service Steering Group met four times: a kick-off meeting on 27 April 2012, a second meeting on 15 May 2012, a third meeting on 4 June 2012 to discuss the draft impact assessment report submitted on 13 June. A fourth meeting took place on 11 October 2012 to discuss the draft impact assessment report before re-submission on 15 October 2012. Before and after the meetings, written contributions and comments on the draft impact assessment were sent by the services.

The key questions addressed to the Member States and to the private sector in the context of all the relevant consultations listed above concerned the need to improve NIS across the EU. To this end, the Commission consulted on the need to foster cooperation at EU level; the importance of building up a minimum common level of national capabilities to enable such cooperation; the pros and cons of requiring the private sector to share information with the public sector and to adopt state-of-the-art protection measures; the establishment of such requirements at EU or national level.

Stakeholders' views on the seriousness of the problem and the options to address it are reported throughout this impact assessment where appropriate.

In general, the respondents to the public consultation:

[5] Final report: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/daa12-final_report_1.pdf

- Expressed the view that governments in the EU should do more to ensure a high level of NIS (82.8% of respondents)

- Expressed the view that users of information and systems are unaware of the existing NIS threats and incidents (82.8% of respondents) and that businesses, governments and consumers in the EU are not sufficiently aware of the behavior to be adopted to minimize the impact of the NIS risks they face (84%).

- Would in principle be favourable to the introduction of a regulatory requirement to manage NIS risks (66.3% of respondents) at EU level (84.8% of those respondents).

- Expressed the view that it would be important to adopt NIS requirements in particular in the following sectors: banking and finance (91.1% of respondents), energy (89.4%), transport (81.7%), health (89.4%), Internet services (89.1%), public administrations (87.5%).

- Expressed the view that 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%).

- 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 (65.1%) and affirmed that also public administrations should be subject to it (93.5%).

- Affirmed that a requirement to report security breaches would not cause significant additional costs (52.5%) and 19.8% said that it would not cause additional costs at all.

In the EFMS and in written inputs to the Commission, the Member States expressed the following views:

- The Commission should develop current NIS actions and mechanisms (Germany, France) especially by means of targeted binding measures (France)

- The development of cyber-security capabilities should be accelerated within the Member States, particularly within the least advanced ones (France)

- That NIS protection levels vary across Europe (Germany) and that there are no mechanisms for engaging in existing cooperation mechanisms with those Member States who are less active in NIS nor are there paths for these Member States to get involved (Estonia).

- An EU framework establishing mechanisms for cooperation on preparedness and response amongst the Member States should be set up (France, Romania, Estonia, Germany, and Finland). In particular:

- Cooperation between the Member States should be underpinned by confidentiality agreements and mechanisms to exchange sensitive data (Spain, Romania).

- Information exchange on good practices and expertise; early warning and crisis management including via cyber-incident exercises should be promoted (Germany, Finland).

- Cooperation should be built on mutual trust (Germany, Finland).

- A functional and effective network of national/governmental CERTs in Europe in which information is exchanged according to the necessary confidentiality standards is needed (France, Romania).

- An approach focused on preparedness and prevention should use harmonized requirements regarding minimum security standards across the EU by maintaining the conditions for fair competition (Germany)

Moreover, the Member States:

– Expressed support for considering the extension of the security provisions in the regulatory framework for electronic communications to new sectors (France) with the appropriate involvement of the Member States in the related discussions (such discussions took place already within the EFMS)

– Expressed support for an EU initiative on NIS covering the ICT sector but also, in a horizontal manner, the ICT component virtually underpinning all sectors (Germany)

– Expressed support for the development of a risk management culture in the private sector (Germany).

The UK questions the merits of a regulatory intervention on NIS at EU level and favours a voluntary cooperation approach facilitated by the Commission. It has particular concerns about the extension of mandatory reporting requirements to sectors other than telecoms.

The **European Parliament Resolution** of 12 June 2012 on "Critical Information Infrastructure Protection: towards global cyber-security[6]" recommends the Commission to:

– "Propose binding measures via the EU cyber incident contingency plan for better coordination at EU level of the technical and steering functions of the national and governmental CERTs";

[6] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167

– "Propose binding measures designed to impose minimum standards on security and resilience and improve coordination among national CERTs"

– "Propose an EU framework for the notification of security breaches in critical sectors such as energy, transport, water and food supply, as well as in the ICT and financial services sectors, to ensure that relevant Member State authorities and users are notified of cyber incidents, attacks or disruptions"

2.3. Impact assessment process

A first version of this impact assessment report was submitted on 13 June to the European Commission Impact Assessment Board and discussed at a meeting convened on 5 July 2012. A revised version of the impact assessment was submitted on 15 October. This new version took into account the various comments from the Board , in particular: a better explanation of the relation between the problem and its cross-border dimension (Chapters 4 and 5); the insufficiency of existing policy measures to solve the problem; the integration of stakeholders' views on various aspects of the problem statement and on all key points of the preferred option; the identification of the sectors and players that would be covered by the preferred option (Chapter 7) and an estimation of the corresponding costs (Chapter 9 and Annexes 2 and 3) that highlighted with more precision the proportionality of the preferred option.

Following the opinion of the Board of 24 October, the following further amendments were made to this impact assessment:

- Insertion of a table showing the extent to which existing obligations address NIS issues and the gaps that still need to be addressed.

- A better explanation of the lack of motivation and incentives for companies and the public sector to invest in NIS (Section 4.1.5.2).

- A description of the nature of the risks in the sectors covered including the extent to which and how networks and services may be affected (Section 4.1.4); strengthening the evidence base and better explaining the rational for the choice of the relevant sectors in the preferred option (Section 4.1.4).

- Additional details on the content of the preferred option (Option 2) and in particular on what NIS risk management requirements would entail in practice (Section 7.2).

- A better explanation of the reasons for not considering other combinations of "soft" and "regulatory" approaches (Section 7.3)

- Improved assessment of social/employment impact, on competitiveness in particular for the preferred option, impact on international cooperation (Section 8 on Assessment of impact of the Options).

- A description and rough estimate of the benefits (i.e. decreasing the cost of NIS incidents and the improved level of security) (Section 9)
- Insertion of a summary table of all costs and benefits per option (Section 9).
- Insertion of a summary of the questions asked and of the responses received in the public consultation (Annex 1).
- Inclusion of the views of stakeholders throughout the text and in the preferred Option.
- Inclusion of the indication of the tools for monitoring and evaluation (Section 10).

3. POLICY CONTEXT IN THE AREA OF NIS

The increasing importance of NIS for our economies and societies was recognised for the first time by the Commission in a Communication from 2001[7] .

The approach adopted so far by the European Union in the area of NIS has mainly consisted in the adoption of a series of action plans and strategies urging the Member States to increase their NIS capabilities and to cooperate to counter cross border NIS problems.

Annex II provides a description of the "Action plans and strategies adopted so far in the field of Network and Information Security in the EU".

Companies, with the exception of telecommunication operators ('undertakings providing public communications networks or publicly available electronic communications services'[8]) and public administrations are not subject to NIS requirements and are not required to report security incidents[9].

7 COM(2001)298

8 See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

9 These consisted of security provisions including on security breaches notifications (Art. 13a&b of Framework Directive 2002/21/EC), and were to be transposed at national level by 25 May 2011

4. PROBLEM STATEMENT

4.1. Problem definition: What is the problem?

The problem can be described as an overall ***insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market.*** The problem is further detailed in the following sections.

4.1.1. Disruptions to the EU internal market

Given that networks and information systems are interconnected and given the global nature of the Internet, many NIS incidents transcend national borders and undermine the functioning of the internal market.

The effects of an incident originating in a particular country, if not appropriately contained, may spread quickly to other countries. Even, incidents that are local by nature may have unforeseen consequences across borders, e.g. the disruption to a major airport's IT systems may affect air traffic across Europe.

Cross-border services can become unavailable, suspended or interrupted due to security breaches. eBay has experienced web-based attacks that have made all or portions of its websites unavailable for periods of time in 2010 and likewise PayPal[10], thereby affecting e-commerce in the internal market.

The case of Diginotar illustrates the risks posed by not reported security breaches. The Dutch certification company Diginotar did not report that its systems were hacked and did not revoke the digital certificates (i.e. the certificates ensuring the security of communications over the Internet) that were fraudulently issued. This resulted in a large number invalid certificates circulating online, compromising the security of Internet services and eventually affecting trust in the Internet. A report[11] by the security firm Fox-IT, which investigated the case, found out that there were a number of problems in the security practices of the company, revealing the need for better risk management and mitigation practises. It must be borne in mind that in the aftermath of the Diginotar incident, the Dutch Government acknowledged that "the risk of security breaches affects the internal market […and] hampers cross-border services and product supplies". For this reason the Dutch Government is preparing a system of mandatory security breach notifications for relevant critical infrastructure and national services[12].

---

[10] eBay Inc. filing to SEC for the fiscal year that ended 31.12.2010 http://www.sec.gov/Archives/edgar/data/1065088/000106508811000003/ebay10k20101231.htm

[11] http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

[12] http://nctb.nl/Images/brief-cyber-meldplicht-en-interventie_tcm91-435018.pdf http://nctb.nl/Actueel/Nieuwsberichten/2012/wettelijke-regeling-meldplicht-en-interventiemogelijkheden-bij-digitale-veiligheidsincidenten.aspx?cp=91&cs=25481

In January 2011, the Commission had to suspend trading in the Emissions Trading System due to security breaches at national registries[13] and companies were prevented from selling and buying emission allowances within the EU.

In the wake of past incidents Member States are starting to introduce their own regulations. As already remarked, the Netherlands are considering introducing security breach notification requirements and Luxembourg[14] has introduced a disclosure requirement for incidents that can have financial consequences for the companies concerned. The UK has taken a sector-specific approach to put in place reporting requirements for critical sectors such as finance, energy, transport and health. Uncoordinated regulatory interventions may result in fragmentation and give rise to Internal market barriers generating compliance costs for companies operating in more than one Member States.

Those businesses which replied to the public consultation emphasised the role that the EU could play in creating a truly integrated and harmonised internal market for NIS products and services and the existence of market barriers which undermine cybersecurity across the EU.

4.1.2. Rising number, frequency and complexity of NIS incidents, and incomplete view of their frequency and gravity

The availability, authenticity, integrity and confidentiality of information and networks can be compromised due to various causes, such as natural events, human errors or malicious attacks.

The outcome of the public consultation confirms the seriousness of the problem, in particular:

56.8% of the respondents reported having experienced over the last year NIS incidents (caused by human mistakes, natural events, technical failures or malicious attacks) which have had a serious impact on their activities.

27.8% of the respondents to the public consultation affirm that human/technical errors are very frequently the cause of NIS incidents, and 39.6% affirm that this is the case quite frequently.

40.8% of the respondents to the public consultation affirm that malicious attacks are quite frequently the cause of NIS incidents.

36.1% of the respondents to the public consultation affirm that software/hardware failure is quite frequently the cause of NIS incidents.

[13] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34

[14] Circular CSSF 11/504 – Frauds and incidents due to external computer attacks

47.3% of the respondents to the public consultation affirm that third party/external failure is quite frequently the cause of NIS incidents.

The flooding of the river Elbe in 2002[15] illustrates how communications systems can be disturbed by a natural disaster. Human error or ignorance can also be the cause of cyber incidents by leading to accidental events. In August 2012 a sub-sea cable was mistakenly snapped between the UK and the Netherlands causing certain Internet Service Providers, e-commerce service providers and customers to be cut off the Internet for more than 24 hours[16]. Incidents of this kind (cable cuts) had already happened in the Mediterranean in 2008 and in the Suez canal in 2011.

The human factor is of the utmost importance for NIS. Non-compliance with security requirements (e.g. by negligence or distraction, using infected USB sticks, opening unsolicited e-mails, failing to apply security patches or revealing passwords) can cause an outage or facilitate the intrusion of malicious software.

The spread of malicious software (malware) and malicious attacks have been increasing steadily. Web based attacks increased by 36% in 2011 compared to 2010 and the total number of attacks by 81%. Malware can mutate as they spread, and attackers are able to generate an almost unique version of their malware for each potential victim[17], which makes their detection ever more challenging. Figure 1 shows the raise in the number of incidents reported to the US-CERT in 2006-2011.

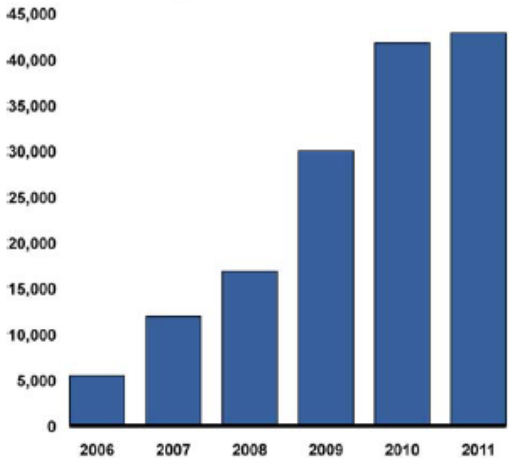


Figure 1: Incidents reported to US-CERT: Fiscal Years 2006-2011[18]

15 http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile

16 http://www.theregister.co.uk/2012/08/28/cut_underseas_cable_cripples_networks/?utm_source=google&utm_medium=twitter&utm_campaign=Feed%253A+InformationSecurityDisclosure+%2528Information+Security+Disclosure%2529

17 Internet Security Threat Report Volume 16, Symantec

18 Cybersecurity, Threats Impacting the Nation, GAO 2012

In addition to the elements presented above, there is reason to believe that a large proportion of attacks go unnoticed. The recent outbreak, in late May 2012, of the 'Flame[19]' cyber-spying software, revealed that malware can be spreading undetected over a number of years. There is moreover reason to believe that only a fraction of incidents, when discovered, are disclosed. The reluctance to disclose comes from the potential significant damages for the organizations involved, including reputational damages and loss of business opportunities.

The lack of information on incidents slows down the capability to react and take the appropriate mitigating measures, in particular in cases where the incident has repercussions outside the organisation and the other parties affected are unaware of an imminent threat or an incident/intrusion that has already taken place.

The most serious of these cross-border incidents may be the state-sponsored stealthy attacks such as 'Shady Rat' etc.[20], where the same techniques are applied in one country then another. Trusted sharing of information about such attacks could help prevent attacks spreading to further countries.

4.1.3. Affecting all actors in the society and economy

Over the last decade, the digital ecosystem has become essential to economic growth and societal welfare. It has enabled the creation of high-quality jobs and supported smart and sustainable economic growth.

Indeed, the ICT sector is one of the growth engines of the EU. In Europe, the ICT sector and investments in ICT deliver around half of our productivity growth. The World Bank estimates that with 10% increase in high speed Internet connections, economic growth would increase by 1.3%. The ICT sector alone represents almost 6% of the European GDP[21].

Public administrations, businesses and consumers reap huge economic and social benefits from the usage of ICT, including online services. Because of the critical role of networks and information systems, possible failures or attacks could impact all parts of society – Member States/governments, organisations/business and citizens/consumers.

---

19 http://www.enisa.europa.eu/media/news-items/The-threat-from-Flamer.pdf

20 http://www.eweek.com/c/a/Security/Huge-Shady-RAT-CyberAttack-Likely-Targeted-Thousands-More-Victims-503656/

21 The Internet economy has generated 21 % of the GDP growth of the last 5 years and could represent as much as 20% of GDP growth in the period up to 2015 in the Netherlands and in the UK. Internet consumption and expenditure already exceed the share of GDP of agriculture or energy, and its GDP is bigger than the GDP of Canada or Spain. It represents 7% of UK GDP, 3.7% in France, 2.2% in Spain, 2% in Italy, 2.7% in Poland, 3.6% in the Czech Republic, 4.3% in the Netherlands, 5.8% in Denmark, 6.6% in Sweden, 3.4% in Germany and 2.5% in Belgium. According to IMRG, in March 2010, 600,000 jobs were associated with e-commerce in the UK.
Each year, 200 million Europeans – 40% of all citizens – buy over the Internet. 27% of European enterprises purchase and 13% sell online. Some sectors have already been profoundly transformed by e-commerce. These include travel agencies (39% of sales took place online in 2008), sales of electronic and cultural goods (22%), financial services, gambling and sports betting (5th Consumer Scoreboard - March 2011).

Security incidents are capable of rendering critical **government functions** unavailable for several days, as demonstrated by the cyber-attacks against Estonia in 2007, which severely affected not only the provisioning of online services such as e-government and e-banking within the country, but also prevented citizens from accessing online services across borders. **EU institutions** have been the target of attacks in 2011 and 2012.

Businesses and other organisations can be seriously affected if the networks and information systems underpinning their industrial processes are compromised. In 2009, 16 % of enterprises in the EU-27 had experienced some kind of NIS incident[22] . Incidents can be costly. The cyber-attacks targeting Sony in April 2011 cost the company nearly $175 million[23]. An outage that affected BlackBerry in 2011 cost the company $50 million[24]. Beginning in July 2009, two U.S. stock exchanges were victims of cyber-attacks[25]. The remote attack temporarily disrupted public websites. In September 2012, six major US banks were hit by cyber-attacks[26]. The loss of intellectual property, trade secrets and financial data ensuing from cyber-attacks also result in considerable losses for businesses concerned. The UK estimates the loss of intellectual property to be largest cost category, accounting for 30% of total losses, resulting from illegal intrusions and cyber-crime, with identity theft and loss of customer data accounting for a much smaller proportion of losses[27].

Consumers can face interrupted e-mailing, instant messaging and browsing services, as it was the case in October 2011, when BlackBerry handsets were affected by a network outage at one of its data centres in the UK and almost all of its 70m users worldwide experienced problems at some point during the three days that the incident lasted[28]. In January 2010, German card holders were suddenly unable to conduct banking or ATM withdrawals and purchases with their bank cards both at home and abroad, due to software problems in the microchips. In the EU, nearly one third of users have already been confronted with a computer virus (or similar infection). Also, 74% of EU Internet users in 2012 think that the risk of becoming a victim of cybercrime has increased in the past year[29]. **82.8% of respondents to the public consultation expressed the view that users of networks and information systems are not sufficiently aware of the level of NIS threats and incidents 84% of the respondents affirmed that businesses, governments and consumers in the EU are not sufficiently aware of the behavior to be adopted to minimize the impact of the NIS risks they face.**

---

22 Source, Eurostat, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ic&lang=en

23 http://www.sec.gov/Archives/edgar/data/313838/000115752311003320/a6733820.htm

24 http://www.sec.gov/Archives/edgar/data/1070235/000107023511000054/pr120211.htm

25 Source, FBI, Statement before the House Financial Services Committee, http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

26 http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?_r=0&adxnnl=1&adxnnlx=1349785139-tC3YxWCWhVImONk4tIKGZA

27 A Detica Report, in partnership with the Office of Cyber security and information assurance in the UK Cabinet Office, 2012 "The cost of cyber-crime".

28 http://www.rim.com/newsroom/service-update.shtml

29 Special Eurobarometer 390/2012 on cyber security http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

4.1.4. Sectors where the well-functioning of network and information security is key to preserve the well-functioning of the internal market

While the problem described above affects all actors of society and economy in the EU, a number of sectors and a number of infrastructure and service providers in those sectors are particularly vulnerable, due to their high dependence on correctly functioning network and information systems and due to their essential role in providing key support services for our economy and society, including health, safety, security and the economic and social well-being of people. As a result, the security of their systems is of particular interest to the functioning of the Internal Market.

The public consultation underlined the importance of ensuring the security of network and information systems, in particular for the following sectors:

- Energy – 89.4% of respondents
- Transport - 81.7% of respondents
- Banking and finance – 91.1% of respondents
- Health – 89.4% of respondents
- Internet services – 89.1% of respondents
- Public administrations –87.5% of respondents

At the same time, **31% of respondents (both business and consumers) to the public consultation affirmed to have no process in place to manage NIS risks. Also, 54.2% affirmed not to have any budget dedicated to NIS.**

All the sectors, which provide services which are key for the functioning of our economies and well-being of our society, rely heavily on network and information systems.

Banking activities should be secured since banks are the backbone of our financial system and because they are common targets of fraudsters. Indeed there are signs that attacks are increasing in this sector. McAfee reported recently[30] that fraudsters, using malware, and replicating the same scheme in several countries, have attempted to steal up to €2 billion from accounts in Europe, the United States and Columbia. Consumers and businesses using online banking have increasingly experienced theft, particularly through viruses infecting their computers. Especially in this sector, we observe an increasing usage of third party business applications (such as those used for mobile banking). These applications, which are often cloud-based, are not part of the network and systems of the credit institution, which has no control over their security.

[30] http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

The stock exchange increasingly adopts networks and information systems and Internet-based commerce systems. Accidental disruptions or malicious attacks affecting the stock exchange in a country or affecting particularly critical stock exchanges such as the ones in London, Paris or Milan may have very significant impact on trade both in the internal market and internationally. In 2010 the London Stock Exchange experienced a serious cyber-attack at its headquarters, which compromised its trading system[31].

Generation, transmission and distribution of energy are highly dependent on secure network and information systems. Ensuring the resilience of utilities is particularly important since virtually all other sectors and the well-being of our society depend upon them.

For example, many major gas companies suffer increased amounts of cyber-attacks motivated by commercial and criminal intent. These attacks are posing a great risk to machinery, which can cost lives, stop production and cause environmental damage.

The same considerations are valid for other network industries, such as air, maritime transport and railways and for key transport infrastructure, such as airports, ports, railways, and traffic management systems and logistics. For example, aviation infrastructure (including ground and in-flight Air Traffic Management) relies on continuous and uninterrupted information flows and databases, which cannot be allowed to fail. Airports and border gateways are dependent on information assurance regarding data, control systems, networks and protocols that support the effective functioning of aviation[32].

Both the energy and the transport sector heavily rely on Industrial Control Systems (ICS), i.e. complex computer and information systems that can be located either in one site (e.g. power plants) or distributed over a geographical area (energy and transport networks).

There are numerous interconnection points between ICS, including over the Internet, and securing them is of the essence. Also, many ICS were designed in the past without anticipating the security threats posed by technological advancements. For example, remote controlling of ICS is often done via simple laptops or other mobile devices which may have a lower level of security than the rest of the system.

The Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids recently concluded in its report to the Commission that "Electricity Critical infrastructures converging with ICT-infrastructures require scenario-building that includes consideration of highly unlikely types of events. ICT security considerations need to be integrated within the wider risk management of the whole grid. ICT is therefore needed to carry out a risk analysis, and to define high level security requirements to enhance the security and resilience of ICT for Smart Grids."[33] Such risk analysis will build upon the positive results of the Commission-led Smart Grids Task Force. The Commission supports the work of the Smart Grids Task Force's Expert

---

31 http://www.cio.co.uk/news/3258814/london-stock-exchange-under-major-cyberattack-during-linux-switch/

32 Source: Centre for Strategy and Evaluation Services, Interim Evaluation of FP7 Research activities in the field of Space and Security, http://ec.europa.eu/enterprise/policies/security/files/doc/aviation_case_study__cses_en.pdf

33 Summary report of the Expert Group on the security and resilience of communication networks and information systems for Smart Grids, July 2012, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm

Group on Privacy, Data Protection and Cybersecurity, where stakeholders from the energy and ICT sectors are developing a cybersecurity assessment framework, which includes the identification of Best Available Techniques (BATs) for smart metering systems as well as the evaluation of methodologies for a trustworthy network sharing vulnerabilities and threats analysis of Smart Grid and Smart Metering systems.
Hospitals and clinics are becoming the more and more reliant on sophisticated ICT systems which need to be secure to ensure continuity of service and avoid fatal disruptions. The proliferation of electronic medical devices presents unique challenges in ensuring that only known, authorized devices are able to connect to the network.
Also, personal health and financial information is often target of cybercrime, particularly as the healthcare industry continues its conversion process to full patient electronic medical records. Networks, mobile devices, workstations, servers and medical devices are particularly critical in this regard and securing them is of the essence.
It is important to ensure the security of Internet companies (e.g. cloud providers, social networks, e-commerce platforms, search engines), which provide key inputs enabling important economic and societal processes. This is essential to preserve trust in the digital ecosystem.
It is key to ensure the resilience and reliability of public on-line services to citizens to build and preserve their trust in e-government. E-Government and e-participation are increasing with citizen demand for timely and cost- effective services and so are the NIS risks for state and local administrations. The risk for public online services to be hindered by NIS problems exist at all levels of government.

Finally, there are NIS problems that are common to all the sectors referred to above. For example, malware is one of the most significant threats as it may disable security or other software in an organisation and cause a breach or a gap that can be exploited by external parties. Also, exposure to threats grows as companies and public administrations invest in technologies like mobile, social, and cloud. Notably, due to the increasing use of mobile devices and applications, employees in virtually all sectors can now access corporate data and look at it remotely without necessarily complying with the security policies and controls of the organisation.

Also, in all the sectors identified above, ensuring NIS in large companies and in SMEs is equally critical. Small and medium businesses have become the low-hanging fruit for cyber criminals and they need to be secure given that we are as strong as our weakest link.
On the other hand, micro companies are less critical for the overall continuity of the services given that incidents affecting them may not have a sufficiently wide reaching impact on society as those incidents affecting larger businesses.

4.1.5. What will happen if further measures are not adopted

4.1.5.1. Undermined consumer confidence in the internal market

The number of NIS incidents and their negative consequences will continue to increase and this will have a negative effect on the use of online public and private services, on consumers' trust in the on-line economy and in the integrity of the Internal Market.

The 2012 Eurobarometer on cyber-security found that 38% of users had concerns with the safety of on-line payments and have changed their behaviour because of concerns

with security issues: 18% are less likely to buy goods on-line and 15% are less likely to use on-line banking[34]. The perceived lack of security on the Internet is thus having a negative effect on the functioning and development of the Internal Market. It is estimated that, by stimulating the development of the digital single market, Europe could gain 4% GDP by 2020[35]. This GDP increase corresponds to a gain of almost €500 billion (€494 billion) or more than €1.000 for every citizen. In a time of economic downturn, this is not negligible.

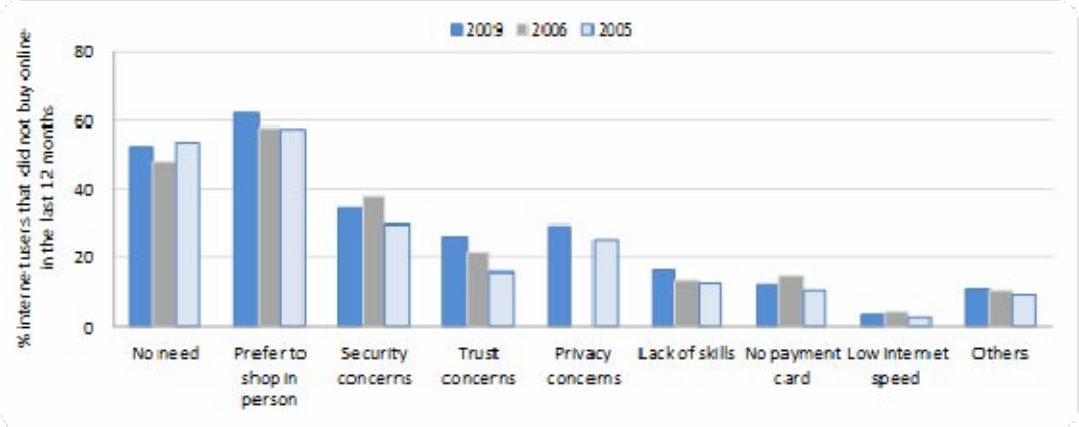


Figure 2: Reasons for Internet users not buying on-line in the EU countries, 2009.
Percentage of individuals with Internet access that did not buy on-line in the last 12 months

4.1.5.2. Insufficient business investments in NIS

Currently, businesses lack effective incentives to conduct serious risk management which involves the adoption of appropriate NIS measures (see also the relevant responses to the public consultation provided in Section 4.1.3). From an economic perspective security is an externality leading to a market failure[36], i.e. market players do not see the economic rationale to bear the full social costs of increasing the level of security but rather prioritise time-to-market or a low pricing for their end products. By leaving the decision on the level of security entirely to market players the societal benefits of a more secure digital environment would not be fully reached.

Often companies consider NIS a purely technical matter and do not address it as a key component of their business strategy, as a lynchpin for safeguarding their most precious assets notably intellectual property, financial information, and their reputation. Companies are often unaware of the risks faced until significant incidents occur and hence only adopt a reactive approach when circumstances require it. The same considerations apply to public administrations which do not yet see the importance of investing in NIS to ensure the continuity and reliability of the public services they provide more and more online.

34 Idem Eurobarometer 390/2012

35 Based on expected GDP for EU27 in 2010 of approximately €12 trillion. Copenhagen Economics, The Economic Impact of a European Digital Single Market, March 2010

36 OECD 2008 'Economics of malware: Security decisions, incentives and externalities' http://www.oecd.org/internet/interneteconomy/40722462.pdf

According to Eurostat[37], by January 2012, 26 % of enterprises in the EU-27 had a formally defined ICT security policy with a plan for regular review; this share rose to over 50 % among those enterprises whose principal activity was information and communication activities. As shown in Figure 3, among the Member States, the highest shares of enterprises with a formally defined ICT security policy were recorded in Sweden and Denmark where more than two fifths of enterprises had such policies. The lowest shares of enterprises with a formally defined ICT security policy were on the other hand recorded in Bulgaria, Hungary, Romania, Poland and Estonia.

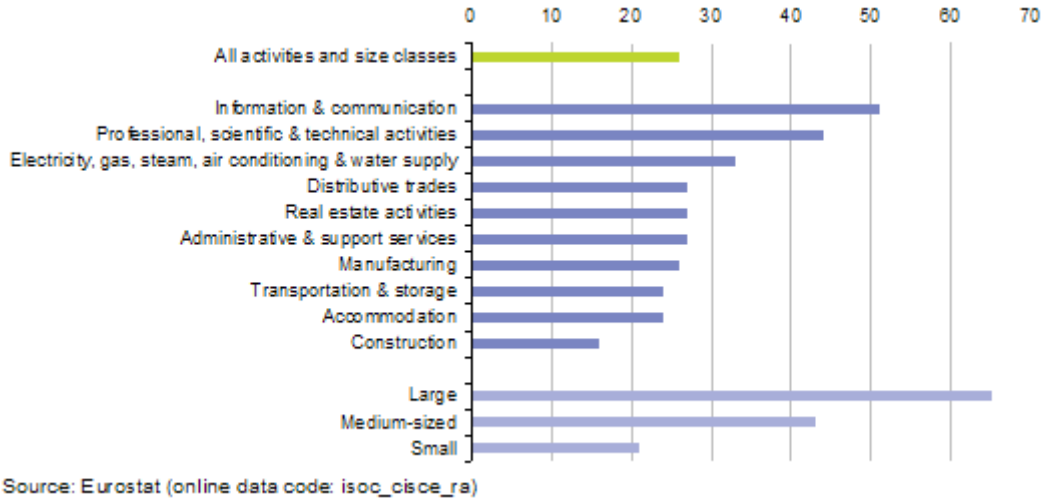


Figure 3 Enterprises having a formally defined ICT security policy with a plan of regular review, EU-27, January 2010 (% of enterprises) - Source: Eurostat [(isoc_cisce_ra)]

Businesses are often unaware of the IT security risks faced and are overconfident about their actual level of protection; they perceive security costs as too high and see no business case for the return on investment on security[38]. Indeed, businesses fail to see the potential savings induced by NIS investments. For example, the Ponemon 2011 Cost of Data Breach Studies for France, Germany and the UK showed that by appointing a Chief Information Security Officer (CISO) businesses could save up to half of the cost of a data breach.

The CSI 2007 Computer Crime and Security Survey found that the majority of companies (61%) allocate 5% or less of their overall IT budget to information security.

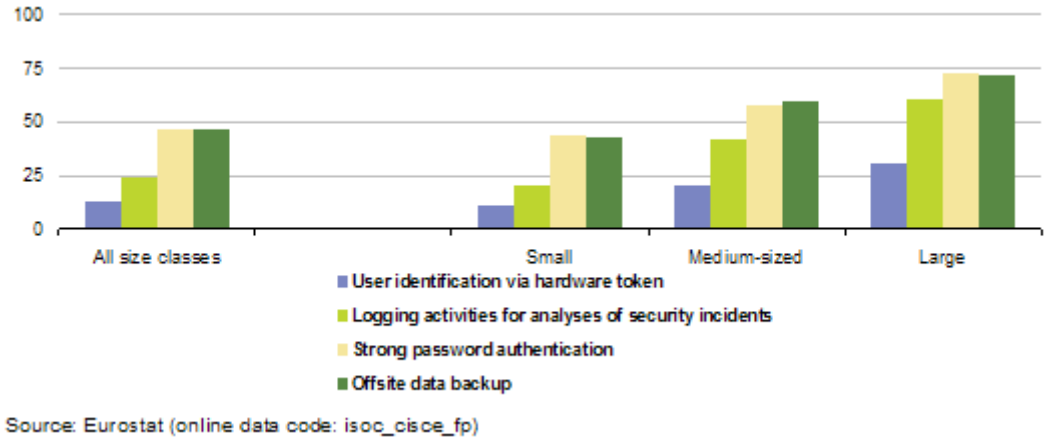
To counter the increasing number of web-based attacks, only 20% of business uses a secure protocol for the reception of orders via Internet[39].

As shown in Figure 4, small and medium-sized companies in the EU adopt less NIS measures than large companies.

37 http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

38 The European Network and Information Security Market, IDC EMEA, 2009

39 Eurostat, Community Survey on ICT usage in businesses, 2008



Source: Eurostat (online data code: isoc_cisce_fp)

Figure 4: Enterprises using internal security facilities or procedures, EU-27, January 2010 (% of enterprises) - Source: Eurostat [(isoc_cisce_fp)]

4.1.5.3. Lack of credibility in the international scene

Without further actions at EU level, the Member States will act individually and will cooperate largely on a bilateral, multilateral or regional level. This would reduce the credibility of the EU at the international level, which would lead to the decay of existing cooperation arrangements, i.e. the EU-US Working Group on Cyber-security and Cybercrime[40] and would hinder discussions with other international partners. This will represent a lost opportunity to coordinate activities at global level and to achieve higher efficiency in addressing the problems.

Furthermore, higher credibility in NIS could boost economic potential and support as such the Internal Market.

4.2. Problem drivers: What is the reason behind the problem?

The problem of insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market stems from a range of factors.

4.2.1. Uneven level of capabilities across the EU[41]

Member States have very different levels of capabilities. This situation hinders the creation of trust among peers in the Member States which is an important prerequisite for

[40] EU-US Summit 2010, Final statement, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597

[41] The information on the state of capabilities provided in this Section is based on the results of the stocktaking exercise carried out by Vice-President Neelie Kroes via two letters sent to Ministries in charge in the Member States respectively in 2011 and in 2012. Not all the Member States have participated to this stocktaking exercise however, the outcomes provide quite a clear overview of NIS capabilities across the EU.

cooperation and information sharing. While research[42] suggests that certain Member States have now reached a high level of spending on NIS, some others have not.

According to a market study[43], Member States can be divided into four groups on the basis of the maturity of their NIS markets:

> Group 1, the Champions: Denmark, Finland, the Netherlands, Sweden, the United Kingdom
>
> Group 2, the Pillars: Austria, Belgium, Germany, Luxembourg, France, Ireland
>
> These two clusters account representing together 69% of the EU GDP but 82% of total security spending. These clusters are characterized by high average security spending, a strong presence of high profile security business users, and greater adoption of advanced security solutions.
>
> Group 3, the Runners Up include the Southern European countries: Cyprus, Greece, Italy, Malta, Portugal, and Spain and: Czech Republic, Hungary and Slovenia.
>
> This cluster shows some delay with the advanced clusters but a good potential for growth. They represent 30% of the EU population, 26% of EU GDP but 16% of the total EU NIS revenues
>
> Group 4, the Learners: Bulgaria, Estonia, Latvia, Lithuania, Poland, Romania, Slovakia,
>
> This cluster includes the remaining Member States with the lowest level of NIS spending and maturity. It represents 5% of EU GDP, but only 2% of NIS revenues) and shows a low number of connected PCs, with very low average security spending per connected PC.

Moreover, important considerations can be made following the stocktaking exercise that VP Neelie Kroes conducted across the Member States. The table below summarises the information provided by the Member States to Vice-President Kroes on their national capabilities. According to the information received, only group 1 countries and a large majority of group 2 countries have a level of preparedness which corresponds to the targets pursued by the Commission since 2009 (CIIP Action plan and CIIP Communication of 2011).

Group of countries	N/G CERTs	CERTs EGC[44] group	NIS Strategy	Contingency/Cooperation Plan

[42] Measuring the cost of cybercrime, June 2012, R. Anderson et al. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

[43] IDC EMEA study on the European Network and Information Security Market, April 2009. http://ec.europa.eu/information_society/policy/nis/docs/others_pdf/smart2007005_D_7_1.pdf

1 - DK, FI, NL, SE, UK	DK, FI, NL, SE, UK	DK, FI, NL, SE, UK	DK*, FI, NL, SE, UK	DK, FI, NL, SE, UK
2 - AT, BE, DE, FR, IE, LU	AT, BE, DE, FR, IE*, LU	AT, DE, FR,	AT, DE, FR, IE, LU	AT, DE, FR, LU
3 - CY, GR, IT, MT, PT, ES, CZ, HU, SL	CY*, GR, IT*, MT, PT*, ES, CZ, HU, SL	ES, HU	CY, EL, ES,CZ, HU	CY, EL
4 - BG, EE, LV, LT, PL, RO, SK	BG, EE, LV, LT, PL, RO, SK		EE, LV, LT, PL, RO, SK	EE, LV

* In the process of adoption

4.2.1.1. Preparedness

Public sector players dealing with NIS in the EU include a large variety of ministries, agencies and National Regulatory Authorities[45]. The existence of a plethora of bodies, each with different competences and responsibilities, makes it difficult for the Member States to identify their counterparts with whom to cooperate in other Member States. Not all the Member States have an operational national/governmental **CERT** in place to handle NIS incidents and prevent them from happening by monitoring threats. This uneven level of preparedness hinders cooperation on a European scale, as confirmed by a study undertaken by ENISA in 2012[46].

The European Government CERTs (EGC) group, which performs operational tasks, comprises only 10 Member States, which are the top performers. As indicated in the group's website[47]: "Its members effectively co-operate on matters of incident response by building upon a fundament of mutual trust and understanding due to similarities in constituencies and problem sets".

Only some Member States have to date adopted national **cyber security strategies.**

4.2.1.2. Response

Not all Member States have in place a **cyber-incident contingency/cooperation plan**, providing protocols for communications and coordinated action in crisis situations, and

44 Informal European Government CERTs Group

45 For overview see ENISA Who-is-Who Directory on network and information security http://www.enisa.europa.eu/publications/who-is-who-directory-2011. See also Annex 4 to this Staff Working Paper.

46 http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012

47 See http://www.egc-group.org/

not all the Member States have carried out or regularly carry out **cyber incident exercises**, which are major tools to put in place and test response capabilities.

All the Member States, supported by ENISA, have participated in the first pan-European cyber-incident exercise in 2010 (Cyber Europe 2010[48]). According to the evaluation report of the exercise, the communication protocols differ from one Member State to another and there is hence a need for harmonisation of the existing communication processes, which also need to be made more secure[49].

In any serious crisis situation affecting networks and information systems, an appropriate response is vital and time critical. When threats or incidents have potential or actual cross border-nature, they need to be handled by the Member States in a coordinated and timely manner.

4.2.2. Insufficient sharing of information on incidents, risks and threats

Most security breaches go unreported and unnoticed mainly due to the reluctance of companies to share this information because of fear of reputational damages or liability. Often, people responsible for NIS share related information only with small groups they trust rather than going through official channels.

The insufficient sharing of information on threats and risks results in sub-optimal preparedness; the insufficient sharing of information on incidents results in sub-optimal response. The unavailability of reliable data and information on NIS threats and incidents makes it difficult for governments to conduct evidence-based policy making and to respond to incidents affecting governments' networks timely.

The lack of NIS data and information does not allow conducting appropriate analysis and compiling statistics that could be used to raise awareness of the rising threats and to plan appropriate measures to tackle them.

There is currently also no framework for trusted information sharing on security threats, risks and incidents amongst the Member States and between the private and the public sector. The UK stressed that mandatory reporting of security breaches may be a disincentive for those governments and businesses that are highly advanced in terms of NIS and that already pursue voluntary and cooperative arrangements. The UK would also favour a sector-specific approach to NIS given that risks and impact of incidents may differ from one sector to the other.

38% of respondents (both business and consumers) to the public consultation considered that effective sharing of information on threats and incidents would be best achieved by a requirement to report significant NIS security breaches to the national competent authority while 37% considered that it would be best achieved by stronger public-private cooperation mechanisms.

---

48 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1459

49 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report

5. EFFECTIVENESS OF EXISTING MEASURES

5.1. There are loopholes in the existing regulatory framework

The only sector where companies are currently required under EU law to take NIS risk management steps and to report serious NIS incidents is the electronic communications sector[50].

The regulatory framework for electronic communications[51] requires providers of public electronic communications networks and services to appropriately manage the risks posed to the security of their networks and services to prevent and minimise the impact of security incidents on users and interconnected networks. It requires providers to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. These provisions had to be transposed at national level by 25 May 2011.

However, all players relying on network and information systems face security risks. This leads to an uneven playing field since the same incident affecting for example a telecommunications provider and a company providing voice over IP services would have to be notified to the national competent authority in the former case, but not in the latter.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[52] requires controllers of personal data to implement appropriate technical and organisational measures to protect personal data. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected. In 2012, the Commission proposed a major reform of the EU legal framework on the protection of personal data[53]. Article 30 of the proposed General Data Protection Regulation[54] requires the data controller and the data processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. The controller and the processor shall, following an evaluation of the risks, take security measures to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in

---

50 Respondents to the public consultation stressed that the financial industry is already required to manage NIS risks under certain national laws, e.g. in the UK, Netherlands and Germany. This would be accompanied by an obligation to report incidents to the national central bank or to the supervisory authorities. It may also be expected that those requirements will be further aligned as part of the plans to establish a European Banking Union

51 Directive 2002/21 a common regulatory framework for electronic communications networks and services (Framework Directive), Article 13 a) and b) as introduced by Directive 2009/140/EC http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf

52 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

53 See http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

54 COM(2012) 11

particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

All players who are data controllers (e.g. a bank or a hospital) are hence already obliged to put in place security measures that are proportionate to the risks faced. On the other hand, data controllers would only be required to notify only those security breaches compromising personal data. A NIS breach affecting the provision of the service without compromising personal data (e.g. an ICT outage of a power company which results in a blackout) does not have to be notified.

The co-legislators are currently discussing the Commission proposal for a Directive on attacks against information systems[55]. The proposed Directive focuses on penalising the exploitation of cybercrime tools. This proposal covers only the criminalization of specific conducts, but does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact.

Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection[56] covers the energy and transport sectors. According to the Directive, the Member States had to go through a process of identifying potential European Critical Infrastructures (ECIs), with the help of the Commission if needed. The Directive also requires operators of identified European Critical Infrastructures to put in place security plans The Directive does not put obligations on operators to report significant breaches of security and does not set up mechanisms for Member States to cooperate and respond to incidents. To date, only few European Critical Infrastructures have been identified as such by the Member States. The vast majority of the energy and transport players (e.g. airports, ports, electricity generators and gas distributors) are not covered.

In sum, the current rules do not require businesses other than telecommunication companies to adopt security measures and report NIS incidents, which do not affect personal data. The Diginotar case referred above illustrates the limits of this approach. Another striking example is the BlackBerry outage in 2011, which caused interruptions in basic communications services such as e-mail and SMS but did not have to be reported since the company is not a telecommunications operator and the incident did not compromise personal data.

Annexes 9 and 9 present the outcome of two specific benchmarking exercises that directly relate to how different aspects of the problem drivers have been dealt with in other sectors.

More precisely, Annex 8 provides an overview of current (regulatory) incentives for risk assessment and NIS in a number of sectors that strongly depend on NIS for the supply of

[55] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF

[56] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

their services. It is concluded that, in general, such incentives are insufficient in sectors other than the telecoms sector.

Annex 9 identifies and analyses a number of EU Early warning and incident handling networks in sectors other than NIS. These networks are used to share confidential information at EU level. Annex 8 provides useful insights on how such networks have been set up in the absence of mechanisms for effective cooperation at EU level.

5.2. The limits of a voluntary approach

The voluntary approach followed so far has resulted in an uneven level of preparedness and limited cooperation, as highlighted above. As a result the effectiveness of NIS capabilities varies considerably across the EU; cooperation takes place only amongst Member States who are well prepared, the others being left out or choosing themselves not to be involved.

The European Forum for Member States (EFMS) facilitates policy discussions and exchange of best practices between Member States. **The limited remit of EFMS means that the Member States do not share information on incidents, risks and threats within the EFMS nor do they cooperate to counter cross border threats.** The EFMS has no power to require its members to have minimum capabilities in place.

ENISA provides **support and advice** to the Commission and the Member States with a view to improving the overall level of NIS in the EU. ENISA **has, however, no operational powers and, for example, cannot intervene to fix NIS problems**. The external evaluation[57] of ENISA in 2007 concluded that the value added of ENISA is its ability to provide an independent platform at the EU level for stakeholders and experts to discuss and compare problems and solutions regarding NIS and that the consensual view is that ENISA should be a well-established single European voice for security but that it should not be given more powers or an operational role. In addition, it must be borne in mind that there is no guarantee that the mandate of the Agency will be actually renewed after 2013.

The European Public-Private Partnership for Resilience (EP3R) is a platform which facilitates the exchange of best practices among the Member States and ICT companies. **The EP3R has no formal standing and cannot require the private sector to report incidents to the national authorities.** A framework for trusted information sharing and for communicating information on NIS threats, risks and incidents is absent within the EP3R.

It can be reasonably assumed that without providing further directions to existing voluntary mechanisms, and specifically to the EFMS and the EP3R, the interest and the added-value in participating will decrease and this might lead to the possible dissolution of these mechanisms over time.

---

[57] http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

5.3. Approach in other regions of the world

Other regions of the world have adopted initiatives to address issues corresponding to the main problem drivers identified in this impact assessment.

In order to raise the level of security of critical information infrastructures, the US established in 1998 the National Infrastructure Protection Center (NIPC).

The National Cyber-security and Communications Integration Center (NCCIC) is an umbrella organisation set up in 2009 to coordinate national initiatives to address threats and incidents, including the US-CERT, National Coordinating Center for Telecommunications (NCC), the National Cyber-security Center (NCSC), and DHS Office of Intelligence and private sector partners from several ISACs.

Along with setting up dedicated capabilities of this kind, the US launched a series of Information Sharing and Analysis Centers (ISACs) for critical sectors[58] (including electricity, finance, health, maritime, ICT, nuclear, water), with the aim to ensure information sharing on threats and vulnerabilities between public and private sectors. The Industrial Control System Information Sharing and Analysis Center (ICS-ISAC) is the Private/Public center for knowledge sharing regarding Industrial Control System[59] (ICS) cybersecurity.

The lesson learnt from these experiences is that their effectiveness depends on the fact that the private sector shares information with the government and vice versa.

The US approach has inspired countries such as the UK, the Netherlands and Australia in setting up NIS capabilities. Although the US was first to establish a CERT already in 1988, the first government CERTs were established in the late 90's/early 2000's in UK, France, Germany, Netherlands and others and several of these came together to form the European Government CERTs group (EGC).

Regarding the reporting of security breaches, under US law companies are required to report security breaches for critical infrastructures does exist (Data Security and Breach Notification Act of 2012).

As a recent development, the Division of Corporation Finance of the US Securities and Exchange Commission released in 2011 guidance regarding public companies' disclosure obligations relating to cybersecurity risks and cyber incidents[60], due to concerns for the cyber-security risks faced by financial institutions. This shows that the US is now adopting an approach to cyber-security which covers key sectors where protection is essential, such as finance.

---

58 See http://www.isaccouncil.org/

59 ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) Source: US Department of Commerce, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

60 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic4.htm

In Canada, "Industry Canada" is the lead agency for the Communications and Information Technology Sector and is responsible for CIP and emergency management. It has established the sector network – the Canadian Telecommunications Cyber Protection Working Group (CTCP) – to promote industry-to-industry, government-to-industry and industry-to-government co-operation in protecting Canadian networks. Industry Canada and CTCP have also established the Canadian Network for Security Information Exchange (CNSIE) to promote collaboration between a larger community of cyber security stakeholders such as the telecommunications, financial, energy, and vendor communities and government departments.

Regarding operational cooperation, the Organisation of American States has attempted to establish a 'hemispheric contact network' of CERTs but as yet the initiative has not flourished.

In the Asia-Pacific region, APCERT (Asia Pacific Computer Emergency Response Team) is a group of 30+ CERTs, mostly government CERTs. Membership is voluntary.

Japan's CERT capabilities were set up in 1996. JPCERT/CC coordinates with network service providers, security vendors, government agencies, as well as the industry associations and is acting as "CERT of CERTs" in the Japanese community. JPCERT/CC helped to set up APCERT. Also relevant is the Japanese Information-technology Security Center (ISEC) established in 1997 as the public information sharing center for promoting information security in Japan, and the recently created Cyber Security Information Sharing Partnership (J-CSIP) providing a platform among critical infrastructures manufacturers.

In Australia the "Trusted Information Sharing Network (TISN)" is a forum in which the owners and operators of critical infrastructures work together, share information on threats and vulnerabilities and develop strategies and solutions to mitigate risk. It comprises seven critical infrastructure Sector Groups and two Expert Advisory Groups, Communities of Interest (CoI) and a Critical Infrastructure Advisory Council (CIAC).

Stakeholders mentioned the Australian Internet Security Initiative (AISI) as a cost-effective black-listing of IP addresses that are apparently compromised by malware and to dispatch that information to relevant ISPs and their customers.

5.4. Need of EU intervention, subsidiarity and proportionality

5.4.1. The EU right to act – Legal basis

The Union is empowered to adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties (Article 26 Treaty on the Functioning of the European Union - TFEU).

In particular, Article 114 TFEU (former Article 95 EC) allows for the adoption of "measures for the *approximation of the provisions laid down by law, regulation or administrative action in Member States* which have as their object the establishment and functioning of the internal market" (emphasis added). Following the entry into force of the Lisbon treaty, the internal market is among the areas of "shared competence" between the Union and the Member States.

The ECJ held in Case C-66/04 that "*by the expression 'measures for the approximation' in Article 95 EC the authors of the Treaty intended to confer on the Community legislature a discretion, depending on the general context and the specific circumstances of the matter to be harmonised, as regards the harmonisation technique most appropriate for achieving the desired result, in particular in fields which are characterised by complex technical features*." (Paragraph 45).

Furthermore, in the international roaming case C-58/08, the ECJ held that:

"*32. (...) the Community legislature may have recourse to (art. 114 TFEU) in particular where there are differences between national rules which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market (...) or to cause significant distortions of competition (...).*

33. Recourse to that provision is also possible if the aim is to prevent the emergence of such obstacles to trade resulting from the divergent development of national laws. However, the emergence of such obstacles must be likely and the measure in question must be designed to prevent them (...)."

Several EU legislative acts based on Article 114 TFUE are related to NIS, showing that the EU legislator has already recognised the need to harmonise NIS rules to ensure the development of the internal market.

This was, in particular, the case for the ENISA regulation, [61] whose the Internal market legal basis was endorsed by the Court of Justice. The Court recognised[62] that [it] "*was an appropriate means of preventing the emergence of disparities likely to create obstacles to the smooth functioning of the internal market in the area*"[63]; and "*the smooth functioning of the*

---

61 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 077, 13/03/2004, P 1-11).

62 ECJ 02.05.2006, C-217/04, United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union

63 Point 62.

internal market risks being undermined by a heterogeneous application of the technical requirements"[64].

Regulation 460/2004/EC, establishing ENISA, states in Recital 3 that "the technical complexity of networks and information systems, the variety of products and services that are interconnected, and the huge number of private and public actors that bear their own responsibility risk undermining the smooth functioning of the internal market".

The 2010 Commission's proposal aimed at modernising and strengthening ENISA[65], currently under legislative procedure, is coherently based on Article 114 TFEU. As remarked in the Impact Assessment[66] accompanying the recent proposal for Regulation on ENISA "Uneven national policies and practices are a clear disruption of the internal market, due to the clear negative externalities resulting from NIS (inadequate policies impacting markets in other Member States), but also due to the positive externalities of good NIS practices (good practices in one Member State positively impact NIS as a whole, thus creating a clear societal good)".

The disparities resulting from uneven situations across the Member States in terms of capabilities, planning and level of protection, constitute at the same time a barrier to the internal market and justify EU action in cases with cross-border relevance, where coordination at the level of planning and at the level of response, including assistance, are needed.

Furthermore, information asymmetry and lack of transparency in the NIS market risk undermining the supply by market operators and manufacturers of networks, services and products as well as the trust of the users, which is one of the key drivers of the internal market.

Last, but not least, well-functioning networks and systems are essential for the functioning of our economy. Disruptions are increasing in frequency and magnitude undermining achievement of the digital agenda, which would have direct negative consequences for growth and jobs.

5.4.2. Subsidiarity test

Regulatory obligations are required to create a level playing field and close some legislative loopholes. A purely voluntarily approach has resulted in cooperation taking place only amongst a minority of Member States with a high level of capabilities. In order to ensure cooperation encompassing all the Member States it is necessary to make sure that all of them have the required minimum level of capabilities.

European intervention in the area of NIS is justified by the subsidiarity principle, due to the:

---

64 Point 63.

65 Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) of 30 September 2010, COM(2010) 521.

66 SEC(2010) 1126

Cross-border nature of the problem

Given the cross-border nature of NIS threats and problems, a complete non-intervention at EU level would lead to a situation where each Member State is left to only guard its own backyard, with disregard of the interdependence between existing network and information systems. An appropriate degree of coordination among the Member States, on the other hand, would ensure that NIS risks can be well managed in the cross-border context in which they also arise, and therefore respects the subsidiarity principle.

According to a recent study[67]*, differences in security regulations represent a (barrier to operating in multiple countries and to achieving global economies of scale. These differences lead to replication costs (up to 27 times) for pan-European operators. Harmonisation could lead to some economies of scale, but these differences are more or less inherent to the level of discretion enjoyed by the individual Member States regarding security and privacy.*

Harmonising the implementation of regulation aimed at security and consumer protection is seen as an 'avoidable barrier'.

Effectiveness of the actions

Action at EU level would improve the effectiveness (and thus add value) to existing national policies, where they exist, or would facilitate their development.

In addition, it is clear that concerted and collaborative NIS policy actions can have a strong beneficial impact on the effective protection of fundamental rights, and specifically the right to the protection of personal data and privacy. European citizens are increasingly entrusting their data to complex information systems, either out of choice or out of necessity, without necessarily being able to correctly assess the related data protection risks. When incidents occur, they will therefore not necessarily be able to take suitable steps, nor is it certain that the Member States would be able to effectively address incidents with cross-border dimension in the absence of EU-wide NIS coordination. For this reason too, further policy action at the EU level seems to be widely justified.

5.4.3. Proportionality of the approach

The measures in the preferred option do not go beyond what is needed to achieve the objectives and do not impose disproportionate costs, as will be illustrated below.

The costs (see Section 8.2) that according to the preferred option would have to be incurred by those Member States lagging behind to put in place the necessary capabilities are not significant; for the others the costs will be negligible.

The costs for ensuring systematic cooperation amongst Member States according to the preferred option would be small when compared to the economic and societal losses and damages which may be caused by NIS incidents.

67 http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/cost_non_europe/im_e_com.pdf

As to the private sector, should security requirements be set at EU level, they would apply only to some sectors for which the public consultation (see Section 4.1.4) underlined the importance of ensuring the security of network and information systems and markets and in which a serious NIS incident would have a direct and real-time effect on the EU economy and society. In any event, as indicated below, the measures proposed to ensure a basic level of protection would be proportionate to risks faced and hence reasonable and generally corresponding to the interest of the entities involved in ensuring continuity and quality of their services.

Moreover, many of these companies, as data controllers (e.g. banks and social networks) are already required by the current data protection rules to secure the protection of the personal data they control. For these companies the additional costs of the security requirements are likely to be marginal.

6. OBJECTIVES

The general objective is to increase the level of protection against network and information security incidents, risks and threats across the EU.

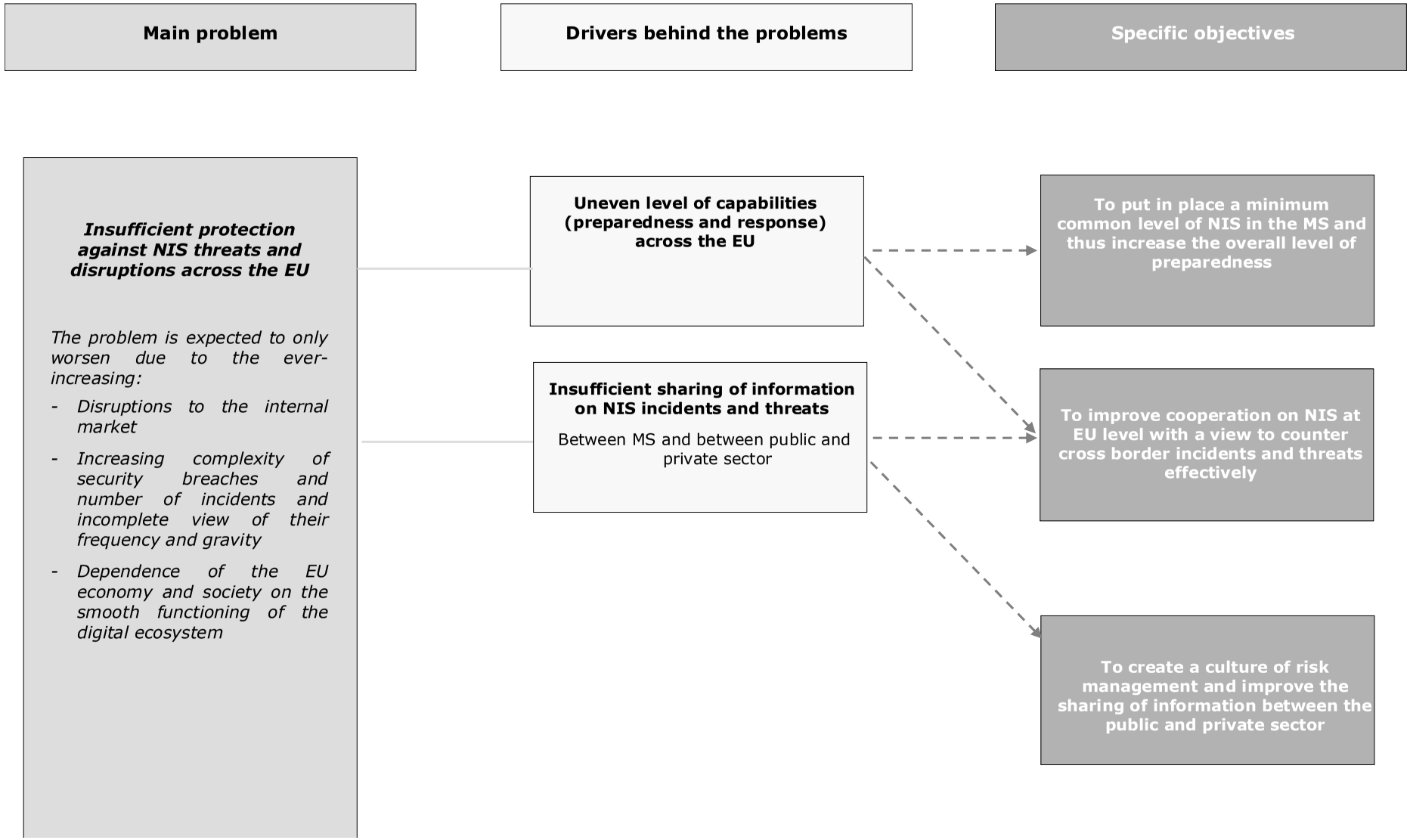
6.1. Overview of general, specific and operational objectives

Specific objectives	Operational objectives
1. To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness and response.	– To ensure that all Member States are adequately equipped at national level both in terms of technical and organisational capabilities to prevent, detect, mitigate and respond to NIS risks, threats and incidents. – To ensure that all Member States develop and update national cyber security strategies and national cyber incident contingency/cooperation plans.
2. To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively.	– To ensure that national competent authorities share NIS information and best practices regularly. – To make sure that such bodies can exchange information cross-border in a reliable and confidential manner.
3. To create a culture of risk management and improve the sharing of information between the private and public sectors.	– To make sure that key private sector players and public administrations engage in

	assessment of the risks and risk management practices. – To ensure that NIS breaches with a significant impact are reported to the national competent authorities.

6.2. Intervention logic

The intervention logic, linking the main problem and the drivers behind this problem to the specific objectives is illustrated in the next figure:


Main problem
Drivers behind the problems
Specific objectives
Insufficient protection against NIS threats and disruptions across the EU
The problem is expected to only worsen due to the ever-increasing:
- Disruptions to the internal market
- Increasing complexity of security breaches and number of incidents and incomplete view of their frequency and gravity
- Dependence of the EU economy and society on the smooth functioning of the digital ecosystem
Uneven level of capabilities (preparedness and response) across the EU
Insufficient sharing of information on NIS incidents and threats
Between MS and between public and private sector
To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness
To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively
To create a culture of risk management and improve the sharing of information between the public and private sector

7. POLICY OPTIONS

The Policy options that have been considered in this Impact Assessment are: Business as usual, Regulatory approach and Mixed approach.

7.1. Discarded Option

The possible Option consisting of ceasing all EU activities on NIS has been discarded.

The Option would imply to stop pursuing the actions under the CIIP action plan and dismantling EFMS and EP3R.

All efforts undertaken in the area of NIS would be left entirely in the hands of the Member States and cooperation would remain limited to a small number of countries, with no virtually mechanisms in place for increasing trust among all of them.

The existing gap between the highly advanced and the less-advanced Member States would likely increase and so would the internal market failures associated to the divergences in the capabilities across the Member States. Such outcomes would not be consistent with DAE "digital single market" and Europe 2020 "smart and sustainable economy" objectives nor would it be efficient or effective for the Member States to tackle NIS cross-border problems on their own.

7.1. Option 1 – Business as usual (‘Baseline scenario’)

Under this Option the Commission, with the assistance of ENISA, would continue with its voluntary approach. With a view to put in place a minimum common level of NIS in the Member States and thus increase the overall level of preparedness and response, the Commission would continue issuing Communications addressing the Member States. Member States would be encouraged to set up well-functioning CERTs and to adopt a national cyber incident contingency/cooperation plan and a national cyber security strategy.

In order to improve cooperation on NIS at EU level, the Commission would recommend to the Member States to establish a network of CERTs across Europe and to adopt a European cyber incident contingency/cooperation plan. The Commission could also dedicate specific funds for building up one or more secure communication network across the EU.

The remit of the EFMS could be expanded to include discussions on the take-up of NIS best practises (e.g. how to best manage risks) by public administrations.

The Commission would also continue to stimulate the creation a culture of risk management and improve the sharing of information between the private and public sector by using platforms such as the EP3R.

Under this Option, ENISA would continue offering its support and expertise to the Member States and to the private sector, for example by issuing technical guidelines and recommendations on NIS capabilities and cooperation.

7.2. Option 2 – Regulatory approach

Under this Option, in order to reach a minimum common level of NIS across the EU and thus increase the overall level of preparedness and response, the Commission would propose to require all the Member States to:

- Set up a well-functioning national/governmental CERT, responsible for handling security incidents and risks according to a well-defined process and complying with essential requirements in terms of mandate and service provided. CERTs would need to have adequate staff and financial resources to carry out their tasks effectively.

- Appoint a national competent authority for NIS which would have a coordination role for NIS and act as a focal point for cross-border cooperation. The authority should be given appropriate technical, financial and human resources and be tasked with the elaboration of the national cyber security strategy (see below). The Member States may decide to have one single body acting both as a CERT and as a competent authority. The CERT would act under the supervision of the competent authority.

- Adopt a national contingency/cooperation plan defining protocols for communication and cooperation among relevant players at national level in case of NIS incidents of a certain scale.

- Adopt a national cyber-security strategy that would outline the strategic objectives and announce the concrete policy actions that each Member State intends to undertake to pursue a high level of NIS.

The establishment of such a common and comparable level of **capabilities** would be a precondition to enable cooperation across the EU.

In order to improve cooperation on NIS at EU level, the Commission would propose to mandate the national competent authorities to form a **network,** together with the Commission, to cooperate against EU level. ENISA would support the competent authorities in their cooperation by providing its expertise and advice.

Within the network the competent authorities would exchange information on serious threats and incidents and would cooperate via coordinated response to counter cross-border threats and incidents. This would occur in organised fashion according to the **European NIS contingency/cooperation plan** that the Commission would adopt following consultation with the Member States via Comitology.

The competent authorities would also ensure timely and regular publication on a common website of non- confidential information on on-going significant threats and incidents and on the coordinated responses adopted.

To build capacity and knowledge in the Member States, the competent authorities would within the network exchange best practices assist each other in building NIS capacities, organise regular peer reviews and pan-European NIS exercises.

The exchange of sensitive and confidential information between the competent authorities would take place through an infrastructure ensuring security and confidentiality.

The Member States would be able to access this secure infrastructure following a decision of the Commission to be taken by means of delegated acts and following assessment that the minimum NIS capabilities at national level described above are in place. The transposition/implementation period would allow the necessary delays for the Member States to comply with the requirements on national NIS capabilities.

Under this Option the Commission would also propose to impose NIS risk management and reporting requirements on public administrations (e.g. central ministries, local authorities, land registries) and key private players thus creating a comprehensive framework to stimulate the creation of a culture of risk management and improve the sharing of information between the private and public sectors. More specifically, the Commission would propose that operators in specific critical sectors, i.e. banking, energy (electricity and natural gas), transport, health, enablers of key Internet services and the public administration, be required to assess the risks they face and to adopt appropriate and proportionate measures to dimension the actual risks.

A detailed list of the entities that would be covered is provided at the end of this Section. An estimation of the actual number of those operators is provided along with the cost assessment in Annex 3. **Micro companies** (i.e. companies with less than 10 employees[68]) would in any case **not be in the scope** of these obligations.

This requirement mirrors the one set out in Article 13a&b of the Framework Directive for electronic communications and would hence contribute to ensure a level playing field.

In order to give an indication of what this requirement may entail in practice, the ENISA guidelines on the security measures in Article 13a of the Framework Directive[69] can be taken as a sample. The activities that could fall under this requirement are:

- **Regular risk analysis** of specific assets for example information, software, physical assets, services and people. A number of standard methodologies exist for performing risk assessments, such as for example the ISO 27005 standard.

- **Governance and risk management** including establishing and maintaining an appropriate security policy; a governance and risk management framework to identify and address risks; an appropriate structure of security roles and responsibilities.

[68] Micro, small and medium enterprises are defined based on the criteria set out in EU recommendation 2003/361

[69] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-for-minimum-security-measures-v1.0

- **Human resources security**, i.e. adopting security measures to enhance the security of personnel such as employees, contractors and third-party users. This may include background checks; ensuring that personnel have sufficient knowledge and follows regular trainings; a process for handling security breaches committed by employees.

- **Security of systems and facilities**, that may include establishing and maintaining physical and environmental security of facilities; security of supplies and supporting facilities such as electric power, fuel or cooling; appropriate (logical) access controls for access to network and information systems; appropriate security of network and information systems.

- **Operation management**, i.e. security of operation and management of network and information systems. This may include establishing and maintaining operational procedures and responsibilities and asset management procedures in order to verify asset availability and status.

- **Incident management,** i.e. establishing and maintaining standards and procedures for managing incidents. This may include establishing capabilities for detecting incidents and forwarding them to the appropriate departments within an appropriate time frame; processes for incident response and escalation; incident reporting and communication plans.

- **Business continuity management,** i.e. monitoring, testing and auditing of network and information systems, facilities and security measures, for example including policies for testing network and information systems.

Moreover, the entities indicated above would be required to report incidents with a significant impact on the services provided[70]. This would also be in line with Article 13a&b of the Framework Directive.

These entities would have to report to the national competent authorities those incidents seriously compromising the operation of networks and information systems and thus having a significant impact on the continuity of services and supply of goods which rely on network and information systems.

For example, an incident affecting an e-commerce platform and preventing the conclusion of on-line transactions over several hours would have to be reported. Likewise, a maintenance incident of an information system of a power plant, which results in stopping the distribution of electricity to a small city during several hours, would also have to be reported. National competent authorities would be empowered to request information, order security audits, issue instructions and carry out investigations on the players covered.

44.4% of respondents to the public consultation expressed the view that a requirement to notify and report incidents to NIS authorities would be needed to make private

[70] In their reply to the public consultation, Finland and GSMA underlined that a reporting obligation would require the competent authorities to have the ability to collect, combine, assess the criticality of notifications and distribute situational awareness on NIS incidents to relevant entities.

companies and public administrations systematically report about cyber security incidents.

57.4% of respondents to the public consultation expressed the view that support from NIS authorities to respond to incidents would be needed to the same purpose.

The reporting of breaches would be tightly linked to the cooperation among the competent authorities at EU level, given that the information fed to them would have to be shared with other competent authorities via the network when it has an actual or potential cross-border dimension. Also, competent authorities would have to prepare annually a summary report on the notifications received that would have to be provided to the Network.

Under this Option, ENISA would continue offering its support and technical expertise to the Member States and to the private sector, for example by issuing technical recommendations and guidelines on capabilities, on EU-level cooperation, on risk management and on the reporting of NIS incidents.

Entities that would be covered by risk management and NIS incidents reporting obligations are (more detailed indications are provided in Annex 3):

- **Energy** (electricity market and gas market):
  - Main electricity generating companies (i.e. those dealing with at least 5% of the country's electricity or gas)
  - Electricity retailers for final consumers
  - Entities bringing natural gas into the country
  - Retailers selling natural gas to final customers

The estimated total number of businesses affected in this sector would be approximately 4000.

- **Transport**
  - Air carriers (Freight and passenger air transport)
  - Maritime carriers (sea and coastal passenger water transport companies[71] and the number of sea and coastal freight water transport companies[72])
  - Railways (infrastructure managers[73], integrated companies[74] and railway transport operators[75])

[71] NACE Rev2 Code 50.1
[72] NACE Rev2 Code 50.2

– Airports (EU airports with more than 15.000 passenger unit movements per year)

– Ports

– Traffic management control operators

– Auxiliary logistics services (a) warehousing and storage[76], b) cargo handling[77] and c) other transportation support activities[78])

The estimated total number of businesses affected in this sector would be approximately 14600.

- **Banking:** credit institutions[79] and stock exchanges

The estimated total number of businesses affected in this sector would be approximately 7706 for credit institutions and 25-30 for stock exchanges.

- **Health sector**: Hospitals including private clinics

The estimated total number of businesses affected in this sector would be approximately 15 000.

- **Enablers of Internet services**

---

73 'Infrastructure managers' are defined as 'Any enterprise or transport operator responsible in particular for establishing and maintaining railway infrastructure, as well as for operating the control and safety systems'.

74 'Integrated companies' are defined as: *'Railway transport operator also being an infrastructure manager'.* Railway transport operators include all public or private transport operators which provide services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term "railway undertaking" is used.

75 Any public or private transport operator which provides services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term "railway undertaking" is used.

76 NACE Rev2 Code 52.1: operation of storage and warehouse facilities for all kinds of goods: operation of grain silos, general merchandise warehouses, refrigerated warehouses, storage tanks etc.

77 NACE Rev2 Code 52.24: loading and unloading of goods or passengers' luggage irrespective of the mode of transport used for transportation – stevedoring - loading and unloading of freight railway cars

78 NACE Rev2 Code 52.29 forwarding of freight, arranging or organising of transport operations by rail, road, sea or air, organisation of group and individual consignments (including pickup and delivery of goods and grouping of consignments), issue and procurement of transport documents and waybills, activities of customs agents, activities of sea-freight forwarders and air-cargo agents, brokerage for ship and aircraft space, goods-handling operations, e.g. temporary crating for the sole purpose of protecting the goods during transit, uncrating, sampling, weighing of goods

79 Credit institutions are defined by the EBC as '*commercial banks, savings banks, post office banks, credit unions, etc.' (see* http://www.ecb.int/press/pr/date/2011/html/pr110114.en.html)

These would include e-commerce platforms, social networks, search engines, cloud providers (Table 8 in Annex 2 provides a thorough indication of relevant players that would be in the scope). Software editors and providers would be excluded. The estimated total number of businesses affected in this sector would be approximately 1400.

- **Public administrations**[80], including local administrations

It should be noted that this represent just an overall indication of the number of businesses that would be in the scope. Annex 3 provides a detail analysis of the process that led to these results.

The importance of ensuring NIS in these sectors has already been highlighted in Section 4.1.4 which also provides the views of the respondents to the public consultation on the importance to set NIS requirements for those who operate in these domains[81].

The same players should engage in NIS risk management and report NIS incidents with a significant impact to national competent authorities.

Only those players operating critical infrastructure and providing vital services relying on ICT significantly would be subject to these obligations. As explained in section 4.1.4 given their dependency on network and information systems, these players are particularly vulnerable to NIS incidents. These sectors are also critical for the economy and society and a serious NIS incident affecting them may produce significant negative side costs and often impair the functioning of the internal market. In many of these sectors a significant "network effect" can be observed, i.e. energy transmission or key online services are by definition provided over a network, the energy grid on the first case and the Internet in the latter. For these reasons the spill-over effects of an incident may be more difficult to contain.

It can be reasonably presumed that most of the players indicated above are, as data controllers, already required under the data protection regulatory framework to implement

---

[80] General government refers to all four sub-sectors of government (see 'Manual on Government Deficit and Debt, Methodologies and Working Papers, ISSN 1977-0375 - Implementation of ESA95' ; URL: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-RA-09-017/EN/KS-RA-09-017-EN.PDF):
These are:
- *central government*: this includes all administrative departments of the State and other central agencies whose competence extends normally over the whole economic territory, except for the administration of social security funds;
- *state government* : this consists of separate institutional units exercising some of the functions of government at a level below that of central government and above that of the governmental institutional units existing at local level, except for the administration of social security funds;
- *local government* : this includes those types of public administration whose competence extends to only a local part of the economic territory, apart from local agencies of social security funds;
- *social security funds* : this includes all central, state and local institutional units whose principal activity is to provide social benefits and which fulfil each of the following two criteria: (1) by law or by regulation certain groups of the population are obliged to participate in the scheme or to pay contributions; (2) general government is responsible for the management of the institution in respect of the settlement or approval of the contributions and benefits independently from its role as supervisory body or employer.

[81] In the public consultation, some stakeholders expressed the view that sectoral regulation in some cases already empowers the regulatory bodies to address security issues. In their views the Commission needs to be careful to avoid unnecessary duplication or contradictions between its proposals and existing mechanisms.

appropriate technical and organizational security measures to protect the personal data they handle. The following players are also data controllers:

- Energy distributors;
- Air, maritime, railway carriers;
- Credit institutions;
- Hospitals and private clinics;
- E-commerce platforms, social networks, booking engines; payment systems; operators of cloud computing platforms (in many cases)
- Public administrations

The table below (Figure 5) shows the extent to which existing obligations address NIS issues and what gaps would be filled by the preferred option.

	Covered by existing EU legislation	**Not covered by existing EU legislation**
Measures to ensure a high level of NIS	Data controllers across all sectors to adopt technical and organizational measures to protect personal data (Article 17, Directive 95/46/EC)	Technical and organisational measures to secure network and information systems beyond the purpose of protecting personal data across all sectors
	Providers of electronic communications networks and services to do NIS risk assessment and risk management (Article 13a&b, Directive 2002/21/EC)	
	Put in place security plans in European Critical Infrastructure in the European Critical Infrastructure in the energy and transport sector (around 20 infrastructure identified so far) (Directive 2008/114/EC)	
Measures to cooperate at EU level	Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States (Article 13a, Directive 2002/21/EC)	Cooperation at EU level among authorities dealing with NIS or among sector-specific authorities sharing information on NIS risks and incidents
	Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in other Member States and ENISA (Article 15, Proposal for Regulation on e-identification and trust services)	
Measures to report NIS	Notification of personal data breaches by data controllers across sectors to the supervisory authority and in specific cases	Notification of security breaches which do not involve breaches of personal data

incidents	to the data subject (Article 31 and 32, Proposal for Regulation on data protection Article 31 and 32)	across sectors
	Notification of personal data breaches by electronic communications providers to the competent national authority and in specific cases to the individual or subscriber (Article 4(3) of e-Privacy Directive 2002/58/EC)	
	Electronic communications operators to notify to the competent authorities breaches of security or loss of integrity with a significant impact on the operation of electronic communications networks and services (Article 13a, Directive 2002/21/EC)	
	Trusted service providers to notify to the competent national body breaches of security of loss of integrity with a significant impact on the trust service provided and the personal data maintained therein (Article 15, Proposal for Regulation on e-identification and trust services)	

Figure 5: Table on existing regulatory gaps

7.3. Option 3 - Mixed approach

Under this Option, the Commission would combine voluntary initiatives based on the goodwill of the Member States, aimed at setting up or strengthening Member State NIS capabilities and at establishing mechanisms for EU-level cooperation, with regulatory requirements for key private players and public administrations on the adoption of NIS risk management measures and the notification of NIS incidents with a significant impact.

With a view to reach a minimum common level of NIS across the EU and thus increase the overall level of preparedness and response, the Commission would encourage the Member States, via Communications or Recommendations, to build **national capabilities** and particularly CERTs**,** to appoint a national competent authorities for NIS, to adopt national cyber incident contingency/cooperation plans and to adopt a national cyber security strategy.

In order to improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively, the Commission would recommend to the Member States to establish a **network of CERTs** across Europe and to adopt a European cyber incident contingency/cooperation plan.

The remit of information sharing platforms such as **EFMS** could be further extended to include in the public policy exchanges taking place therein also public authorities from critical sectors such as banking, energy, transport or health.

These soft measures would be accompanied by regulatory requirements aimed at closing existing regulatory loopholes and create a level playing field across the EU.

In a view to stimulate the creation a culture of risk management and improve the sharing of information between the private and public sector, the Commission would propose to legally require public administrations and key private players in specific sectors (banking, energy - electricity and natural gas -, transport, health, postal services, Internet services and public administrations, see Option 2) to carry out risk management by assessing the risks they face and adopting measures appropriate to meet those risks.

In addition, public administrations and key private players will have to report to national competent authorities those incidents seriously compromising the operation of networks and information systems and thus having a significant impact on the continuity of services and supply of goods which rely on network and information systems.

These regulatory requirements under Option 3 would hence be identical to those imposed under Option 2 both regarding the targeted entities and for the substance of the obligations.

The remit of EP3R could be further extended to include operators from additional critical sectors such as banking, energy, transport or health and continue to be a platform for the exchange of best practices between the public and the private sector.

Under this Option, ENISA would provide support and technical expertise to the Commission, the Member States and the private sector, for example by issuing technical guidelines and the recommendations on capabilities and EU-level cooperation, as well as on the take-up of risk management practises and on reporting security breaches.

This Option could have also been designed in other ways. In particular, it could have combined a regulatory approach for the Member States NIS capabilities and EU cooperation and a voluntary approach for the adoption of NIS risk management and for the reporting of NIS incidents by key private entities and public administrations.

The reason why this alternative combination was not considered is that a voluntary approach to risk management and incident reporting does not work for the reasons given in the Problem statement (i.e. insufficient business investments on security and lack of incentive to share information on NIS risks and incidents despite the worrying threat landscape).

8. ANALYSIS OF IMPACTS

The assessment covers, in addition to the **level of security**, the **economic** and **social impacts** of the three options. It covers also the **costs** which would be incurred under options 2 and 3.

None of the identified options will have impacts on the environment that can be predicted with accuracy.

8.1. Option 1 – Business as usual ('Baseline scenario')

The level of security

Despite the existing policy initiatives, it is unlikely that all the Member States would reach comparable levels of national capabilities and preparedness.

The mechanisms for cooperation and coordination at EU level would remain voluntary. In the absence of a minimum level of national capabilities in all the Member States, there would be no guarantee that cooperation involving all of them would take place. Lack of a framework and an infrastructure for sharing trusted information, based on common confidentiality requirements would also hinder such exchanges at EU level. Cooperation would continue within closed circles of Member States trusting one another. This would increase the gap between the high-performing and less-performing Member States.

The high-performing Member States have the ability to help businesses on their territories in detecting and responding to security incidents and this fosters cooperation between the public and private sector. In less-performing Member States market players' incentive to cooperate with the public sector will continue to be limited.

Only electronic communication providers would continue to be bound to adopt risk management practices and report breaches of security with a significant impact, on the basis of Article 13(a) of the Framework Directive. All other relevant market operators and public administrations would have no incentive to do so, other than purely commercial ones for business. A level playing field would not be achieved and regulatory loopholes would continue to exist.

The lack of a comparable level of security and of cooperation across the Member States may also hinder international cooperation since it would be more difficult to present a common European position on NIS to foreign partners. Instead, non-European NIS stakeholders would have to liaise with the Member States (or just with some of them) on a bilateral basis, with the risk of adoption of different approaches. This would constitute a significant weakness in a domain where international cooperation is essential.

Economic impacts

The impact would depend on the extent to which the Member States would follow the Commission's recommendations. Given the voluntary nature of this approach, the pace of development would vary significantly across the EU. The insufficient level of security in the less developed Member States would undermine their competitiveness and growth by discouraging foreign companies from investing and doing business in these countries.

Given the interdependency of European networks and systems the negative impact of incidents, risks and threats on the EU economy as a whole (and not only in the less-prepared Member States) would increase overtime. Incidents related to NIS would become more and more visible to every business and consumers. This would seriously undermine the confidence in the digital environment and hinder the completion of the Internal Market.

Without improving the overall security framework in the EU we will not be able to reverse the trend of increasing security incidents and minimise their impact. Therefore, this option will come at a cost, which, as indicated in specific examples in the problem statement, is potentially very high.

Social impacts

The continuation and expected aggravation of incidents, risks and threats would negatively affect the online confidence of citizens.

The interests of citizens would be compromised when data are stolen, leaked, abused or corrupted due to a NIS incident, especially as no effective protection would be granted when data do not qualify as personal data.

As more and more critical sectors depend on network and information systems (including health care systems, financial services and significant portions of the public sector), incidents compromising their resilience would undermine the availability of the services provided by these critical sector sand this would cause significant societal harm.

Finally, with no harmonisation of NIS requirements within the Internal Market, employment in the information security industry will be hampered as it may be economically advantageous for European companies to tolerate occasional NIS incidents rather than investing in security, including via hiring and training competent personnel. Employment levels would hence under this Option remain suboptimal.

8.2. Option 2 – Regulatory approach

The level of security

Under this Option, the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably.

The obligations placed on Member States would ensure that all of them are adequately equipped, both in terms of technical and organisational capabilities and preparedness. A common minimum set of requirements would contribute to the creation of a climate of mutual trust, which is a precondition for any effective cooperation at European level.

Secure and effective cooperation at European level would allow coherent and coordinated prevention and response to cross-border NIS incidents, risks and threats.

The introduction of requirements to carry out NIS risk management for public administrations and key private players would create a strong incentive to manage and dimension security risks effectively.

The obligation for public administrations and key private players to report NIS incidents with a significant impact would enhance the ability to respond to incidents and would foster

transparency. The availability of key data and information on NIS would also empower governments to carry out targeted analysis and compile statistics and hence to use reliable information on NIS to set the most adequate priorities in this domain.

The regulatory option, by enhancing the level of security, would enable the EU to demonstrate leadership in the area of NIS and become a more authoritative and effective player in international fora and in talks with its main international partners. By doing this, the EU will be better positioned to export its values and interests, thus also improving the protection of European citizens, businesses and administrations against threats originating outside the EU.

Economic impact

As a result of the increased level of security across the EU security problems would be more swiftly remedied and their impact diminished. The associated financial losses would also be reduced.

These benefits would be felt evenly across the EU, as potential divergences in national policies would be removed thus enabling a level playing field and supporting the development of the Internal Market.

This would improve business and consumers' confidence in the digital world and the Internet and so create new opportunities for business and the digital economy. Users will feel more secure on-line and this will improve their trust in the Internet to the benefit of the Internal Market.

In particular, the promotion of a risk management approach and a security culture would be beneficial to business and public administrations. Carrying out risk assessment would enable and incentivise them to efficiently allocate resources to manage NIS risks and would hence increase the value of the organisation to the public. Also, as businesses in the same sector would be required to implement similar security measures across the EU, businesses would compete on an equal footing.

Organisations would be better equipped to handle incidents and attacks, resulting in enhanced availability, reliability and quality of their services. This would raise the level of trust and satisfaction of those who use those services, increase profits and foster the development of the market. This is particularly important in markets requiring a high level of security for example the one for eHealth applications and the emerging cloud computing market.

The promotion of an enhanced risk management culture would also stimulate demand for secure ICT products and solutions. This would create new markets and opportunities in the EU and capitalise on the European research investments by improving prospects for their commercial exploitation.

Social impact

A higher level of security would improve the on-line confidence of citizens who would be able to reap the full benefits of the digital world (e.g. social media, eLearning, eHealth).

These crucial services would become more attractive due to their improved reliability and availability. This can highly empower citizens in rural or remote regions with limited access to offline services.

Finally, this Option is very likely to boost employment of NIS personnel in the EU due to the requirements to conduct NIS risk assessments and adopt appropriate security measures.

It is worth stressing that according to the "European Social Survey[82]" the EU citizens find it important that governments ensure the safety of citizens against all threats. Moreover in 2010, compared to 2008, it was observed an increase in the percentage of citizens (67.2% against 63.2%) seeing a role for the government to ensure safety against all threats.

Impact on competitiveness

Overall impact on the EU economy

In general, it can be expected that an enhanced availability, reliability and quality of the services offered in critical sectors that rely heavily on network and information systems will be benefit the competitiveness of the EU economy as a whole. For example, the availability of secure platforms for e-commerce and other web-based services could bring important economic benefits and allow a broad range of companies to bring new products and services to the market.

Sectoral competitiveness

Referring to the "Competitiveness proofing" toolkit[83], a distinction can be made between[84]:

- **Cost competitiveness**: the cost of doing business, which includes the costs of factors of production (labour, capital and energy);
- **Capacity to innovate:** the capacity of the business to produce more and/or better quality products and services that better meet customers' preferences;
- **International competitiveness:** the above two aspects could also be assessed in an international comparative perspective, so that the likely impact of the policy proposal on comparative advantages on the world markets is taken into account.

The impact on the competitiveness of the market of ICT security products and services can also be assessed.

82 http://ess.nsd.uib.no/essmd

83 Cf. 'Operational guidance for assessing impacts on sectoral competitiveness within the Commission IA system' (http://ec.europa.eu/governance/impact/key_docs/docs/sec_2012_0091_en.pdf)

84 Cf. "Competitive proofing toolkit" – page 8.

Impact on competitiveness of sectors within the scope of the obligations

The impact in terms of **cost competitiveness** has been quantified[85] in Annex 2 on the compliance costs related to additional risk management measures and in Annex 3 on the administrative burden related to reporting significant NIS breaches. **It can be concluded that the additional costs in general remain limited since many measures have already been taken based on existing regulatory obligations**.

It may be expected that there will be an impact on the **capacity to innovate** of some of the entities within the scope. In some sectors, e.g. eCommerce platforms, booking engines, operators of cloud computing platforms, the new requirements could open opportunities to improve the features of current products or services (cf. *'capacity for product innovation'*).

Finally, regarding **international competitiveness**, this Option would not differentiate between domestic and foreign business operating in the EU. *Competition in the internal market* would be improved by creating a level playing field via an enhanced harmonisation of NIS requirements, improved consistency of NIS risk management measures and coordinated response to incidents, enabled by a more systematic reporting of NIS incidents. For EU-based companies, the risk management measures (e.g. which are likely to result in compliance with international standards) could be considered as a competitive advantage when exporting products and services outside the EU (*competitive advantage in the external markets*).

Impact on competitiveness of ICT security products and service providers

A positive impact is finally also expected for the providers of ICT security products and services. First of all, demand is expected to increase. Furthermore, the development of specific security measures for the sectors within the scope, combined with a better harmonised approach at EU-level, will allow for innovative product development and economies of scale.

8.2.1. Cost estimations

In order to estimate the costs for the Member States to set up national NIS capabilities and participate in EU-level cooperation, it was made use of: 1) indications provided by the Member States during dedicated interviews 2) comparable initiatives and 3) opinions of NIS experts.

In order to estimate the magnitude of the impact on businesses and public administrations, use was made of comparable data provided by Eurostat, in Commission reports on regulated markets and statistics provided by sector-specific federations at European-level.

It must be borne in mind that reliable data on actual investments on NIS is difficult to find, given that companies are generally reluctant to disclose it given its confidential nature. Statistics on NIS expenditure of businesses are similarly scarce. It is difficult to assess how

[85] Approach and data sources used are consistent with the best practice recommendations in the "Competitive proofing toolkit".

much is spent on NIS since it does not generally represent a separate budget line. Indications provided by Gartner[86] were used.

(a) Costs for the Member States associated with building-up NIS capabilities and cooperation at EU level

The costs for NIS capabilities and cooperation would vary across the Member States, according to the respective current level of preparedness.

For the three Member States that have not yet established **national/governmental CERTs** (Cyprus, Ireland and Poland) the estimated cost of putting in place the related infrastructure and services based on interviews carried out with CERTs that are already operational would be **approximately 2.5 million EUR per CERT**.

As regards **NIS competent authorities**, it is likely that Member States would choose to designate existing bodies as competent authorities and assign additional tasks to these bodies. The corresponding additional costs should be regarded in terms of Full-Time Equivalents (FTE). Those Member States which have a sufficiently staffed authority in place would incur no additional costs.

Assuming that an average of 6 FTE per Member State (based on consultations with several national NIS bodies) would be required to carry out the tasks of a competent authority (i.e. developing and implementing a **cyber-incident contingency/cooperation plan** and a **national cyber security strategy**) the average cost would be **360 000 EUR per Member State**. The total theoretical maximum cost would be **9.72 million EUR across the EU** and de facto lower, since a few Member States already have co-ordinating cyber security centres or bodies in place.

As regards **pan-European cyber-incident exercises**, the first Cyber Europe exercise coordinated by ENISA in 2010 created an operational cost of 150 000 EUR for ENISA, with future exercises being expected to cost around 300 000 EUR. A total of 150 experts from the Member States were involved in 2010. Assuming that each expert dedicated two fulltime months on average to the exercise, the exercise would have required the equivalent of 25 FTE or a total of 1.5 million EUR for all the Member States per pan-European exercise and 750 000 EUR for all the Member States per year, assuming that a pan-European exercise takes place every two years. This would mean a cost **per Member State of 55 555 EUR per exercise**.

The costs related to the cooperation among the competent authorities within the **network** would be limited to travel and subsistence expenses, only when travelling would be required. Assuming two participants per Member State and three meetings per year with an average cost of 1000 EUR for travel and subsistence, the cost **per Member State** would stand at approximately **6000 EUR per year**.

The costs related to the common website where the competent authorities would timely and regularly publish non-confidential information on threats, incidents and response adopted would amount to a **setup cost of 5000 EUR** (estimating that it would take 25 days and 2/3 technician and 1/3 project manager to setup the website including meetings, specifications,

[86] http://www.gartner.com/technology/home.jsp

visual design, implementation, going online). This would be an EU-average manpower cost[87]. On a recurrent basis, the cost would be 200 EUR/month[88] and hence **2400 EUR/year** for the EU (this would cover among the others hosting and domain name).

The costs for carrying out tasks linked to this website, e.g. providing content and promoting the website, would be covered by the costs for the competent authorities that have been illustrated above.

The costs for establishing the **physical infrastructure** necessary for the sharing of information in the Network of competent authorities and CERTs would depend on whether the Member States would decide to use an existing infrastructure or to set up a dedicated one.

The cost of the physical infrastructure would depend on whether the Member States would choose to use and adapt an existing infrastructure (e.g. sTESTA[89]) or to establish a new one. In the former case it has been estimated that the cost would be **about 1 million EUR** (based on the cost for the adaptation of the system that was developed by the JRC for the early warning and response system in public health) and can be borne by the EU budget, budget line 09.03.02 (to promote the interconnection and interoperability of national public services on-line as well as access to such networks - Chapter 09.03, Connecting Europe Facility – telecommunications networks) on condition that funds are available under the Connecting Europe Facility (CEF); alternatively, the related costs would have to be shared among the Member States. In the latter case (setting up of a new infrastructure) the related cost has been estimated to be **10 million EUR** per year for the EU as a whole (this is the cost currently incurred by the Commission in relation to sTESTA, which is provided by the French network operator Orange) and would have to be shared among the Member States.

(b) Compliance costs for public administrations and key private players

The additional NIS spending that would be required has been calculated as the difference between the target level of spending according to current best practices and the current actual spending in the various relevant sectors (taking into account the estimated annual natural increase in spending due to rising NIS threats).

The target level adjusted by the natural increase in spending is 6.61% of a company's total IT spending.

The total additional NIS compliance costs would hence be in the range from **1 to 2 billion EUR**.

This estimation takes into account that most of the entities affected are already supposed to be compliant with existing security requirements, namely the obligation for data controllers to take technical and organisational measures to secure personal data, including NIS measures. Thus, the present Option would primarily entail new efforts and costs for entities which do not qualify as data controllers.

87 Assuming a cost of 150 EUR for a technician and of 300 EUR for a project manager.

88 Considering that one man*day/month (2/3 technician, 1/3 project manager) should suffice

89 http://ec.europa.eu/idabc/en/document/2097.html

The costs have been hence reduced by a certain factor to take into account existing spending on security.

Given that the magnitude of this reduction is hard to estimate with precision, different scenarios are taken into account, namely the numbers in bold in table 5 indicate the total additional costs when a 70% cut is applied (left column) and when a 40% cut is applied (right column), respectively.

	Range of additional ICT spending required, caused by NIS Regulation (Compliance cost of the NIS Regulation)					
	Per sector		Per company		in % of turnover	
	Mill EUR		EUR			
Energy	0,0	0,0	0	0	0,000%	0,000%
Transportation	118,0	236,0	8.084	16.168	0,032%	0,064%
Banking and financial services	170,0	340,0	21.975	43.951	0,023%	0,047%
Healthcare providers	67,4	134,7	4.501	9.003	0,023%	0,045%
ICT sector (excl. telecom)	4,4	8,9	3.238	6.476	0,015%	0,030%
TOTAL (excl. public sector)	**359,8**	**719,6**			in % of OPEX	
Public sector	577,4	1.154,8			0,026%	0,052%
TOTAL	**937,2**	**1.874,5**				

Table 5: Estimated additional spending for compliance with NIS risk management obligations

As regards SMEs[90] , they are the back-bone of the European economy as they constitute more than 99% of all European businesses.

A considerable number of these companies are micro-enterprises, i.e. companies which employ less than 10 people. They have been excluded from the scope since they do not have the scale nor do they provide the services that would fall within the scope of the requirements. Also, NIS incidents affecting micro enterprises and a consequent discontinuity of the services offered by these companies may not have a sufficiently wide reaching impact on society as those incidents affecting business of larger size. For this reason, regulatory measures on these players would not be justified.

However, there are small (up to 50 employees) and medium enterprises (from 50 to 250 employees) to which the requirements would apply.

Starting from the total compliance costs for the private sector (see Table 5), which range from 360 to 720 million EUR, the compliance cost **per small and medium enterprise** would fall in the range of **2500 and 5000 EUR**. In carrying out the calculation, it has been assumed that

[90] Micro, small and medium enterprises are defined based on the following criteria (cf.: EU recommendation 2003/361):

Company category	Employees	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

small and medium enterprises account for 20% of the turnover of the private companies concerned by the regulation and represent 68% of all the companies affected or just over 28 000 enterprises.

This is the estimated average cost per SME for achieving the current level for 'best in class' in terms of NIS protection. As technologies evolve the risks on the one hand and the protection measures on the other hand will continue to evolve as well. Continuous investments to keep up with the state of the art will thus be required but it is very difficult at this stage to foresee what the costs involved in keeping up with technological developments will be. These investments will, however, ensure that both large and small enterprises and the European economy will be well positioned to reap the benefits of the global cyber security market, which is projected to be among the fastest growing segments of the Information Technology (IT) sector in the next 3 to 5; the cyber security market was in 2011 worth $63.7 billion, and is expected to grow to between $80 and $120.1 billion by 2017[91].

Annex 3 provides a detailed indication of the entities involved, their turnover or operating expenditure, and the additional costs that would have to be borne.

Regarding costs that would have to be borne by SMEs, Annex 4 provides the SME-test.

(c) Costs for public administrations and key private players associated with reporting NIS incidents with a significant impact

In order to value the costs for reporting serious NIS incidents, an estimation of the notifications that would be done over one year has been extrapolated from existing data on the implementation of Article 13a of the framework directive for electronic communications. On this basis, the number of NIS incidents notifications expected would amount to approximately 1700 per year. Assuming that one employee would have to devote 0.5 working day for the notification, and that the notification as such would have a negligible costs (e.g. it would be done via an e-mail) the **expected cost per breach notification would be 125 EUR**, leading to a **total cost for notifying breaches on an annual basis of 212 500 EUR at the EU level**.

Regarding possible investigations that can be initiated by the NIS competent authorities on the compliance with risk management and NIS incidents notification obligations, it is not possible at this stage to estimate if and how many investigations could be initiated. It can however be reasonably assumed that 10 to 20% of the NIS incidents notifications might be followed by an investigation, corresponding to an absolute value of 170 to 340 expected investigations per year.

Taking into account the standard salary cost, the maximum cost for the entity affected would be **maximum 25 000 EUR per investigation** or **4.25 million to 8.5 million EUR per year across the EU**.

The costs for the annual reporting on notifications that the competent authorities would have to prepare and deliver to the Network would already be included in the costs indicated above for the Member States to adequately staff and equip the competent authorities.

[91] Cyber-Security Market - Global Forecast & Trends (2012 – 2017), http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html and Global Industry Analysis Inc "Cyber Security - A Global Strategic Business Report"

A detailed analysis of the process that led to these estimations is provided in Annex 4.

8.3. Option 3 – Mixed approach

The level of security

Under this Option, it is unlikely that all the Member States would reach comparable levels of national capabilities and preparedness via voluntary initiatives.

As a consequence, in the absence of a minimum level of national capabilities in all the Member States, there would be no guarantee that cooperation involving all of them would take place.

Given that also mechanisms for cooperation and coordination at EU level would remain voluntary, cooperation would continue within closed circles of Member States trusting one another. Lack of a framework and an infrastructure for sharing trusted information, based on common confidentiality requirements would also hinder exchanges at EU level. This would increase the gap between the high-performing and less-performing Member States.

On the other hand, the introduction of security requirements for public administrations and key private players would create a strong incentive for those players to manage and dimension security risks effectively. These mechanisms would however be ineffective in those Member States who would not follow the Commission recommendations on the setting up of NIS capabilities. For example, without a national competent authority being appointed, there would be no organisation or body to which NIS incidents could be reported.

Also, it is unlikely that public administrations would be able to carry out appropriate NIS risk management in those Member States where NIS capabilities would not be in place at the level of the central government (e.g. CERT or national competent authority).

Overall, under this Option the EU would miss an opportunity to increase the general level of NIS, as progress would still be patchy.

The lack of a comparable level of security and of cooperation across the Member States would harm the effectiveness of international cooperation as described in the assessment of Option 1. This would constitute a significant weakness in a domain where international cooperation is essential.

Under this Option, the EU as a whole would not demonstrate leadership in the area of NIS and not be well position to export its values and interests.

Economic impacts

Given the voluntary nature of this approach, the pace of development would vary significantly across the Member States. The insufficient level of security in the less developed Member States would undermine their competitiveness and growth by discouraging foreign companies

from investing and doing business in these countries. Also, the less performing Member States would be more exposed to the negative impact of incidents, risks and threats.

The public administrations and the private sector would adopt measures to remedy problems more swiftly and to dimension their impact. However, given the continuing weakness of certain Member States, the overall level of security in the EU would remain low and hence the impact of incidents, risks and threats on the EU economy would increase overtime.

Without securing the weakest link, incidents would become more and more visible to business and consumers. This would undermine the confidence in the digital environment and hinder the completion of the Internal Market.

The regulatory requirements on public administrations and key private players would however stimulate demand for secure ICT products and solutions. This would also create new markets and opportunities in the EU and capitalise on the European research investments by improving prospects for their commercial exploitation.

Social impacts

The continuation and expected aggravation of incidents, risks and threats would negatively affect online confidence, especially in those Member States which do not regard NIS as a priority.

Although the NIS requirements for key private players and public administrations could generate the social benefits described in the assessment of Option 2 in terms of increased use of digital technologies, citizens' empowerment and boost of employment, the likely disparities in the Member States' approach to NIS would generally hinder such benefits.

Finally, this Option is very likely to promote employment of NIS specialised personnel in the EU due to the requirements to conduct NIS risk assessments and to adopt appropriate security measures in a number of sectors.

Costs

The costs for setting-up national NIS capabilities and for the cooperation at EU level will depend on the extent to which the Member States would conduct these activities on a voluntary basis.

The compliance costs for public administrations and market operators will be identical to those described above under Option 2.

9. COMPARING THE OPTIONS

9.1. Overall comparison of the assessment

The previous chapters presented a detailed assessment of the three selected policy options.

Given the urgency to enhance the level of protection against NIS incidents, threats and vulnerabilities as described above, and the need to implement the policy objectives that are proposed in this impact assessment to address the problem drivers, it must be concluded that Option 1 and 3 are not to be considered viable for reaching the policy objectives and are therefore not recommended, given that their effectiveness would depend on whether the voluntary approach would actually deliver a minimum level of NIS and, regarding Option 3, it would depend on the good will of the Member States to set up capabilities and cooperate cross-border.

Option 2 is the preferred one given that under this Option the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably. In particular, the obligations on Member States would ensure adequate preparedness at national level; the setting up of coordinated mechanisms at EU level would deliver EU-wide coherent and coordinated prevention and response; the establishment of common NIS requirements for public administrations and key private players would foster a strong culture of risk management and would curb information asymmetry in the market. Moreover, by putting its own house in order the EU would be able to extend its international reach and become an even more credible partner for cooperation at bilateral and multilateral level. The EU would hence also be better placed to promote fundamental rights and EU core values abroad.

Annex 13 specifies the extent to which each policy option contributes to the achievement of the objectives. The assessment of the impacts under each of the options was done by analysing the *magnitude* of the expected impact, as well as the *likelihood* that the impact will actually occur as a result of the proposed policy option. According to these criteria Policy Option 2 has scored the highest in achieving the objectives.

9.2. Overall cost-benefit analysis

The table below (Figure 6) provides an overview of the costs related to each of the 3 policy options. The Table shows that Option 2 would entail the highest costs as a consequence of the regulatory approach. Costs stemming from Option 3 would be slightly lower as the Member States' spending for NIS capabilities and for participating in EU cooperation will depend on the goodwill of each Member State. The table also shows benefits for each option, as explained in the assessment of the options presented in the previous Section.

	Option 1 Business as usual	Option 2 Regulatory approach	Option 3 Mixed approach
a) Costs related to setting-up national NIS capabilities and participation in EU cooperation			
Setting up of national/governmental CERT	**Between 0 and 7.5 million EUR** (Depending on the precise capability it is the MS without CERT would develop with no obligation to do so)	**Approximately 2.5 million EUR per CERT per year** (for the three MS not having a CERT yet (Cyprus, Greece and Malta), 0 EUR for the MS already having a CERT in place)	**Between 0 and 7.5 million EUR** (Depending on the precise capability it is the MS without CERT would develop on a voluntary basis)
Establishing Competent Authorities	N/A	**Maximum 9.72 million EUR (360 000 EUR per MS) per year** (For the EU 27, this figure stands on average six additional FTEs per MS to be added in an existing organisation)	**Between 0 and 9.72 million EUR** (Depending on the precise capability it is that would be developed on a voluntary basis)
Set-up of common website for the publication of non confidential information on NIS threats	N/A	**5 kEUR** (set-up cost for the website) **2.4 kEUR** (yearly recurring cost for the website)	**Between 0 and 5 kEUR** (set-up cost) **Between 0 and 2.4 kEUR** (yearly recurring cost) (Depending on the intention of the MS to develop and maintain a voluntary website of this kind)
Cooperation of competent authorities within a network	N/A	**6 kEUR per MS per year** (On yearly event costs relates to travelling and subsistence, assumption of 3 meetings per year and two participants per MS per meeting)	**6 kEUR per MS per year** (Depending on the degree of additional cooperation that would be put in place on a voluntary basis)
Participating to pan-European exercises	**750 kEUR for all MS per exercise** **(or ± 28 kEUR per year per MS)** (For the EU 27, this figure relates to the participation of 150 experts, involved during two months for an exercise every two years)	**750 kEUR for all MS per exercise (or ± 55.5 kEUR per MS per exercise)** (For the EU 27, this figure relates to the participation of 150 experts, involved during two months for an exercise every two years. It is also assumed that the increased cost of a future increase of the scope of the exercises would be compensated by an increased efficiency).	**750 kEUR for all MS per exercise** **(or ± 28 kEUR per year per MS)** (For the EU 27, this figure relates to the participation of 150 experts, involved during two months for an exercise every two years)
Establishment of the physical infrastructure ensuring secure information exchange	N/A	**Around 1 million EUR** for adapting sTESTA (borne by EU if funds are available under CEF or cost shared among the Member States) or **10 million EUR per year** for a new dedicated network comparable to sTESTA (cost to be shared among the Member States)	**N/A** (It is assumed that the establishment of an EU wide *physical* infrastructure would not be realised on a voluntary basis)
b) Compliance costs for public administrations and key private players (related to NIS risk management measures)			
Adoption of additional risk management measures	N/A	**1 to 2 billion EUR** in total (per year for all sectors considered) **6.5 kEUR to 44 kEUR** on average per company, depending on the sector **2.5 to 5 kEUR** per SME within the scope of the Regulation	**Idem Option 2**
c) Administrative burden for public administrations and key private players (related to reporting NIS incidents with a significant impact)			
Reporting on incidents with a significant impact	N/A	**125 EUR** per breach notification **Maximum 25 000 EUR** per investigation	**Idem Option 2**
	Competitiveness and growth not ensured; risk of undermining citizens' interests and critical services; decreased confidence of citizens; employment hampered; difficulties in presenting a common EU position internationally	Swift remediation of incidents and reduced related costs; enhanced trust in the digital economy and in the internal market; creation of market for security solutions; enhanced competitiveness; enhanced citizens' opportunities and employment; EU more authoritative internationally	Competitiveness and growth not ensured; overall risk that citizens' interests and critical services will be undermined and that on the confidence will decrease; employment opportunities enhanced; creation of a market for security solutions

Figure 6: Comparative table of costs for the three Policy options

An overall cost-benefit analysis would require a quantification of the possible benefits of compulsory measures to ensure a high level of NIS across the EU. Some of these benefits can

be directly linked to fact that NIS incidents would have no or little impact when NIS measures are in place. Other benefits are more general and relate for example to the effects of increased confidence in the digital economy.

Assessing the magnitude of the possible benefits in this particular context is extremely difficult for a number of reasons and in particular given that:

- There is an incomplete view of the frequency and gravity of NIS incidents;
- There are general indications that the number, frequency and complexity of NIS incidents are on the rise. However, there is no information on the pace of this increase nor are there sufficient quantitative elements available on how the situation is today so to estimate the absolute magnitude of this increase;
- It is difficult to assess to what extent enhanced NIS would mitigate the negative impact of security incidents.

Some of the measures proposed (especially those on the reporting of NIS incidents) are meant, at least to some extent, to address this lack of data. Beside the positive effects on trust in the digital economy and the internal market, the main benefits of this option will stem from the likely contribution to decreasing the costs of security incidents, including malicious attacks. The following estimates indicate the scale of these actual or potential costs:

- According to the World Economic Forum, in the next ten years there is a 10% likelihood of a major Critical Information Infrastructure breakdown with potential economic damages of over $250 billion.
- The global consumer cybercrime is estimated at **100 billion US $ worldwide** (per year); there are moreover clear indications that cybercrime is starting to focus their efforts on the increasingly popular platforms such as social networks and mobile devices[92].
- The cost of cyber-crime in the UK, related to Intellectual Property (IP) theft and industrial espionage, was estimated by Detica[93] at **21 billion £ per year.** The cost of cyber-crime for government was estimated at **2.2 billion £ per year** (total cost of tax and benefits fraud, local government and central government fraud, national health services (NHS) fraud and pension fraud). The study furthermore stresses that the full economic impact goes beyond the direct costs that were identified in the study.

10. MONITORING AND EVALUATION

This Section proposes measures to monitor and evaluate the impact of the preferred option, on the basis of the three specific objectives that such Option aims at achieving.

92 See http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02

93 See 'The Cost of Cyber Crime' – a Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.

First of all, the Commission would periodically review the functioning of the legislation particularly on the basis of technological and market developments and would provide a report to the European Parliament and the Council every three years.

The review process would also be supported by targeted studies, information received from the Member States, expert discussions, workshops, Eurobarometer statistics, etc.

The core indicators and tools in the table below provide a general framework for monitoring and evaluation.

Core indicators of progress towards meeting the objectives:

Specific objectives	Monitoring indicators	Tools
1. To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness.	• Number of Member States having appointed a NIS competent authority which is adequately staffed and equipped to carry out EU-level cooperation • Number of Member States having established national/governmental CERTs which meet the pre-defined minimum baseline requirements • Number of Member States having adopted a national cyber-security strategy • Number of Member States having adopted a national Cyber incident contingency/cooperation plan	• Surveys of competent authorities • Comparative implementation reports on national cyber security strategies, the role of competent authorities, functioning of CERTs and national cyber security contingency/co operation plans
2. To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively.	• Number of competent authorities cooperating via the network • Number of competent authorities participating in the secure information	• Surveys of competent authorities • Progress report on the implementation of the European cyber

	exchange • Information exchange among the competent authorities on NIS incidents, risks and threats • Implementation of the European cyber incident contingency/cooperation plan • Reduced divergence of Member States' approaches to NIS • Number of NIS cyber incident exercises at EU level • Number of conferences/meetings between Member States to define commonly agreed goals for NIS • Capacity building activities involving the Member States • EU-wide NIS practices • Collection of comparable data on NIS by the competent authorities • Regular and timely publication of non-confidential information on threats, incidents and response on a common website	incident contingency/co operation plan • Assessment of the outcome of capacity building activities involving the Member States (e.g. based on country case studies)
3. To create a culture of risk management and improve the sharing of information between the private and public sectors.	• Regular NIS risk assessment by public administrations and key private players • Level of investments in	• Survey of players within the scope of NIS requirements to assess the level

	NIS by public administrations and key private players • Number of notifications of NIS incidents with a significant impact to the competent authorities (the sum of this number and the number of public administrations and companies which have failed to notify security breaches should be decreasing over time) • Governments' access to information and data on actual NIS incidents (on the basis of the notifications received) and possibility to carry out analysis and compile statistics and to set priorities on NIS accordingly	of NIS investments and the best practices adopted to ensure NIS • Surveys of competent authorities to evaluate the incidents notifications received (incl. e.g. case studies and peer reviews assessing in more detail the reporting obligations put in place in the Member States • Comparative implementation report on the criteria applied for defining a significant breach

ANNEX 1: PUBLIC CONSULTATION ON NETWORK AND INFORMATION SECURITY ACROSS THE EU

SUMMARY OF ANSWERS RECEIVED

An online public consultation ran from 23 July to 15 October 2012.

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).

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

The questions posed in the online public consultation focused on:

- **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.

- **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.

- **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.

Regarding the **Scale of the problem and evidence on impact**, most of the respondents (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%), software/hardware failure (36.1%) and human/technical errors (27.8%).

Regarding **Improving NIS through an EU strategic approach,** a very large majority (82.8%) of the respondents 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, a large number of respondents affirmed that those could entail support from NIS authorities to respond to incidents (57.4%), notification and report to NIS authorities (44.4%) and publicity of incidents and establishment of performance ranking (44.4%). Only 8.9% of the respondents affirmed that no incentives are needed in this regard.

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 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.

Avery large majority of respondents (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%).

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%).

The majority of respondents would also in principle be favourable to the introduction of a regulatory requirement to manage NIS risks (66.3%) at EU level (84.8% of those respondents). 70.5% of those respondents also suggested that this requirements entail a general obligation to adopt state of the art measures proportionate to the risks identified.

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 incentives for effective information sharing on threats and incidents, the respondents suggest to establish a requirement to report significant NIS breaches to the national competent authority (37.9%) or to establish stronger public-private cooperation mechanisms (37.3%).

The majority of the respondents (65%) eexpressed 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.

ANNEX 2: ACTION PLANS AND STRATEGIES ADOPTED SO FAR IN THE FIELD OF NIS IN THE EU

In its Communication "Network and Information Security: Proposal for A European Policy Approach" of 2001, the Commission outlined the increasing importance of NIS for our economies and societies[94]. As part of its response to security threats, the European Community decided in 2004 to establish the European Network and Information Security Agency (ENISA)[95] to ensure a high and effective level of NIS in the EU. The role of ENISA is to contribute to the development of a culture of NIS for the benefit of citizens, consumers, enterprises and public sector organisations in the European Union and to provide advice to the European Commission to this effect. A Commission proposal to update and extend ENISA's mandate is under discussion in the Council and European Parliament[96].

In 2006, a Strategy for a Secure Information Society[97] was adopted in response to the urgent need to coordinate efforts for building up trust and confidence of stakeholders in electronic communications and services. Already the 2006 Strategy ambitioned to further develop a dynamic, global strategy in Europe based on a culture of security and founded on dialogue, partnership and empowerment. The main elements of this strategy were endorsed in a Council Resolution[98].

The Commission adopted, also in 2006, its proposal for a "European Programme for Critical Infrastructure Protection (EPCIP)"[99] which sets forth the overall "umbrella" approach to the protection of critical infrastructures in the EU. One of the EPCIP implementation actions is Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection[100] that covers the energy and transport sectors.

The Safer Internet Programme[101] 2009-2013 was launched in 2008 and provides a strong foundation to promote safer use of the Internet and other communication technologies, particularly for children, and to fight against illegal content and harmful conduct online.

After an intensive process of consultation with all relevant stakeholders, the Commission adopted, on 30 March 2009, a Communication on Critical Information Infrastructure protection (CIIP)[102] focusing on the protection of Europe from cyber-attacks and cyber disruptions by enhancing preparedness, security and resilience. The Communication launched an action plan with five pillars of actions: preparedness and prevention; detection and

---

94 COM(2001)298

95 See Regulation (EC) No 460/2004 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-CELEX:32004R0460:EN:HTML

96 COM(2010)521 e

97 COM(2006)251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf

98 2007/068/01

99 COM(2006)786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

100 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

101 Decision No 1351/2008/EC http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2009/decision_en.pdf

102 COM(2009)149 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

response; mitigation and recovery; international cooperation; criteria for the ICT sector. The CIIP Action Plan put forward, for the ICT sector, the necessary sector-specific policies complementing the overall European Programme for Critical Infrastructure Protection (EPCIP).

The Action plan was endorsed in the Presidency Conclusions of the Ministerial conference on CIIP in Tallinn in 2009. These commitments were further advanced by the Council Resolution on "A collaborative European approach to network and information security"[103] adopted on 18 December 2009.

The revised regulatory framework for electronic communications[104] in force since November 2009 set new security provisions including on security breaches notifications (Art. 13a&b of the Framework Directive), that were to be transposed at national level by 25 May 2011.

Security and resilience issues are notably addressed under the Trust and Security chapter of the Digital Agenda for Europe[105], one of the flagship initiatives of the EU2020 Strategy. In particular, Key action 6 of the Digital Agenda for Europe calls for measures aimed at a reinforced and high level NIS policy.

The Digital Agenda for Europe is complementary to other initiatives such as the Stockholm Programme for Freedom, Security and Justice and the Internal Security Strategy in action (ISS)[106]. The Stockholm Programme/Action Plan[107] and the ISS underline the Commission's commitment to building a digital environment where every European can fully express his or her economic and social potential.

More recently, the Commission second Communication on CIIP of March 2011 on "Achievements and next steps: towards global cyber-security"[108] took stock of the results achieved since the adoption of the CIIP action plan in 2009 and described the next priorities planned under each action both at EU and at the international level. Council Conclusions on CIIP were adopted on 27 May 2011[109]. The 2011 CIIP Communication contains a number of actions in which the Commission calls upon the Member States to set up NIS capabilities and cross-border cooperation. Most of these actions should have been completed by 2012, but as highlighted in Section 4.2.1, they have not been yet implemented.

---

103 2009/C 321/01

104 See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

105 COM(2010)245,http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf

106 COM(2010)673 lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

107 COM(2010)171 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF

108 COM(2011)163 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

109 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccybersecurity_/sede150611cccybersecurity_en.pdf

Discussions are also on going as regards the Commission proposal for a Directive on attacks against information systems[110] which aims at harmonising the criminalisation of specific conducts.

Recently, the Commission adopted a Communication[111] on the establishment of a European Cybercrime Centre (EC3), which would be part of Europol and act as the focal point in the fight against cybercrime in the EU. EC3 is intended to pool European cybercrime expertise to support Members States in capacity building, provide support to Member States' cybercrime investigations and become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

At the international level, since the 2010 EU-US Summit[112], a joint EU-US Working Group on Cyber-security and Cybercrime has been established.

The EU is also active in relevant international multilateral fora, such as the Organisation for Economic Co-operation and Development (OECD), the United Nations General Assembly (UNGA), the International Telecommunication Union (ITU), the Organisation for Security and Co-operation in Europe (OSCE), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF). The EU also actively participates to the London process on cyberspace.

A revised CIP policy package is foreseen for adoption in the coming months. The objective is to review EPCIP, including Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

110 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF

111 COM(2012)140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF

112 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm

ANNEX 3: ASSESSMENT OF NIS RISK MANAGEMENT COMPLIANCE COSTS FOR PUBLIC ADMINISTRATIONS AND KEY PRIVATE PLAYERS

Introduction

Assumption taken regarding the scope of relevant costs

All public administrations and key private players would under Option 2 and 3 be required to conduct risk assessment and to put in place risk management measures proportionate to the risks faced.

As in the electronic communications sector, the threshold for significance could be defined in relation to the impact that the breach may have on the operation of networks or services. A very important aspect in this regard is the *perspective of the consumers or citizens* that could be affected, and this is something that will vary from sector to sector. For example, for hospitals, this threshold would not relate to the number of patients that could be affected (size of the hospital), but to the seriousness of a possible breakdown of the network and information systems for a single patient, e.g. in case a crucial medical system goes down during surgery. Taking into account this criterion and for each of the sectors presented below, an assessment is provided of the number of companies affected and the financial impact on them. Micro-companies would be excluded.

Methodology for the cost assessment

- STEP 1: Identification of relevant sectors (based on Scope of Options 2 and 3) incl. estimation of their revenues/turnover
- STEP 2: Identification of the cost related to ICT security spending that is currently not yet made 'naturally' by the organisations and which can be considered as 'underinvestment'
- STEP 3: Assessment of the additional cost for risk management that could be caused by NIS risk management obligations .

STEP 1: Identification of relevant sectors and entities, incl. turnover

In the following, an estimation is made of the number of entities that are expected to be impacted by the risk assessment obligations, as well as of their turnover (so as to be able to make further calculations in the following steps). The exercise is done for each of the following sectors separately:

- **Energy market** (electricity market and gas market)
- **Transport sector** (operators of air transport, rail transport and maritime transport; incl. auxiliary logistic services)
- **Financial sector** (all credit institutions and stock exchanges)

- **Health sector** (hospitals)
- **Enablers of Internet services** (excl. telecom operators already within the scope of the Telecom Framework Directive)
- **Public administrations**

It should be noted that results presented below should be treated with caution, i.e. the goal is to obtain an overall idea of the **type and number of entities** and subsequently of the order of magnitude of the impact.

Energy market

The energy market can be further subdivided in the electricity and gas market. More precisely, the actors within the scope of the risk management requirements are:

- Electricity generating companies
- Electricity Transmission and Distribution System Operators (TSO and DSO)
- Entities bringing natural gas into the country
- Gas Transmission and Distribution System Operators (TSO and DSO)

Recent data on the number of these companies in the EU is not yet available in the Eurostat dissemination database, but can be found at:

http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Electricity_market_indicators

http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Natural_gas_market_indicators

Furthermore, the DG ENERGY 'Report on progress in creating the Internal Gas and Electricity Market' (2009-2010) also gives some indications of the number of Transmission System Operators (TSOs) and Distribution System Operators (DSOs): http://ec.europa.eu/energy/gas_electricity/legislation/doc/20100609_internal_market_report_2009_2010_annex.pdf.

As for the generating companies, only the 'main' companies (those dealing with at least 5% of the country's electricity or gas) are considered to be particularly critical. Possible problems in energy supply by smaller generators due to NIS breaches will easily be tackled by other companies, thus not resulting in a significant impact. For retailers, the situation is different, as a breach in NIS for one company can have a direct significant impact on its customers, regardless of the size of the company. Therefore, all electricity and gas transmission and distribution operators are assumed to be relevant for inclusion. This leads to a **total number of businesses affected**, equal to **approximately 4000**:

	ELECTRICITY SECTOR			GAS SECTOR			
	Number of main electricity generating companies	Number of Transmission System Operators (TSO) - Electricity	Number of Distribution System Operators (DSO) - Electricity	Number of main entities bringing natural gas into the country	Number of Transmission System Operators (TSO) - Gas	Number of Distribution System Operators (DSO) - Gas	Total number of companies
	2010	**2009**	**2009**	**2010**	**2009**	**2009**	
Belgium	3	1	26	3	1	18	52
Bulgaria	5	1	129	1	1	28	165
Czech Republic	1	1	3	3	1	79	88
Denmark	2	1	84	2	1	3	93
Germany	4	4	866	7	18	695	1.594
Estonia	1	1	38	1	1	26	68
Ireland	6	1	1	6	1	1	16
Greece	1	1	1	3	1	3	10
Spain*	4	1	351	5	14	22	397
France	1	1	148	3	2	25	180
Italy	5	9	144	3	3	263	427
Cyprus	1	1	1	0	1		4
Latvia	1	1	11	1	1	1	16
Lithuania	5	1	2	4	1	6	19
Luxembourg	2	1	6	1	1	4	15
Hungary	3	1	6	6	1	10	27
Malta	1	0	1	0	1		3
Netherlands	5	1	8		1	10	25
Austria	4	3	129	4	7	20	167
Poland	5	1	20	1	1	6	34
Portugal	2	3	13	2	1	11	32
Romania	6	1	36	2	1	38	84
Slovenia	2	1	1	2	1	18	25
Slovakia	1	1	3	3	1	46	55
Finland	4	1	88	1	1	23	118
Sweden	5	1	170	2	2	5	185
United Kingdom	8	1	20	7	4	20	60
EU27	**88**	**41**	**2.306**	**73**	**70**	**1.381**	**3.959**

Table 1: Overview of number of affected businesses in the electricity and gas sector per MS

To estimate the revenues of these businesses, an extrapolation is made with the help of another data source, namely Eurostat structural business statistics. Whereas this source provides for information at the level of the much broader 'electricity, gas and water supply sector'[113], it is useful to derive a unitary value for the average turnover of a company in the sector, which can then be extrapolated to the volumes presented above. More precisely, with the help of the Eurostat figures an average turnover per business is derived by dividing the total[114] sector turnover by the number of enterprises in the sector:

113 See Eurostat, Structural business statistics, NACE_R1 Code E comprises *'Electricity, gas and water supply'* and is the best proxy available for estimating the average turnover of electricity and gas companies.

114 Only taking into account medium-sized and large enterprises, i.e. micro- and small enterprises do not intervene in the calculation as they are considered not relevant for inclusion in the scope (cf. the broad definition of the NACE_R1 code E comprising around 28.000 companies whereas only electricity and gas generating and retailing companies are targeted here).

in mill EUR	Companies with from 50 to 250 persons employed	Companies with 250 persons employed or more	Total (over 50 persons employed)
Turnover	137.308	544.205	681.513
Number of companies	2.120	960	3.080
Average turnover per company	65	567	221

Table 2: Estimation of average company turnover (based on NACE_R1 Code E)

This average turnover per business resulting from the Eurostat data is then combined with the total number of businesses as presented in the table above (i.e. 3959 companies), leading to a total turnover at the EU level of 876 billion EUR (visible in summary Table 11).

Transport sector

The relevant activities within the transport sector relate to those for which a significant NIS incident would have some kind of 'network effect' impacting other actors in the sector, resulting easily in a wide spread impact, incl. cross border, and thus impacting an important number of customers (citizens as well as businesses).

Based on this criterion, operators in the air, rail and maritime transport sector are considered to be key operators that would fall within the scope of the obligations (both infrastructure owners and operators/service providers over these infrastructures), and this for both passenger and freight transport. As for freight transport, next to the transport companies *stricto sensu*, also companies providing auxiliary logistics services (such as warehouse operating and cargo handling), irrespective of the mode of transport, should be included in this scope, as they are an equally vital part in the time-critical transport flow of goods. To define the number of companies active in each of these subsectors in the EU, the following sources were used:

Air transport:

- In terms of infrastructure, Eurostat provides for statistics on the number of main airports in the EU (with more than 15 000 passenger unit movements per year): http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=avia_if_arp&lang=en

- As for airlines, Eurostat also has information on the number of companies active in passenger air transport[115] and freight air transport[116], but for passenger air transport these figures do not only include commercial airlines, but also e.g. operators of scenic and sightseeing flights, thus resulting in a very high overall figure that is not representative for the EU market targeted. The Eurostat figures per Member State are therefore only taken into account for freight air transport, and for passenger air transport use is made of a general indication of the size of the market by DG TREN

115 NACE Rev2 Code 51.10
116 NACE Rev2 Code 51.21

(see factsheet on the sector http://ec.europa.eu/transport/air/doc/03_2009_facts_figures.pdf), and the number of passenger air operators at the EU level that is provided by them is further distributed over the individual Member States according to the distribution of freight air transport companies.

- Traffic control for air transport is usually not provided by the operator/owner of the infrastructure, so that these types of companies form a separate category for the air transport subsector. Information on the number of companies could not be found, but revenue data is reprised below.

Railway transport:

- Number of railway operators in the EU can be found in Eurostat (total of infrastructure managers[117], integrated companies[118] and railway transport operators[119]): http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=rail_ec_ent&lang=en

Maritime transport:

- For the number of 'operators' on the market, Eurostat provides information on the number of sea and coastal passenger water transport companies[120] and the number of sea and coastal freight water transport companies[121] per Member State.

- As for the infrastructure, i.e. the ports, DG MOVE states there are about 1 200 ports in the EU[122], and by lack of readily available data per Member State, this total is distributed over the individual Member States according to the distribution of freight maritime transport companies (this does not influence results for the EU total, but has as a consequence that the data at Member State level should be treated with caution).

Auxiliary logistics services:

---

117 'Infrastructure managers' are defined as 'Any enterprise or transport operator responsible in particular for establishing and maintaining railway infrastructure, as well as for operating the control and safety systems'.

118 'Integrated companies' are defined as: *'Railway transport operator also being an infrastructure manager'.* Railway transport operators include all public or private transport operators which provide services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term "railway undertaking" is used.

119 Any public or private transport operator which provides services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term "railway undertaking" is used.

120 NACE Rev2 Code 50.1

121 NACE Rev2 Code 50.2

122 http://ec.europa.eu/transport/maritime/ports_en.htm

- The EU statistical system has a separate section on 'warehousing and support activities for transportation', of which a) warehousing and storage[123], b) cargo handling[124] and c) other transportation support activities[125] seem most relevant, i.e. excluded are support activities to land, water and air transportation as they contain elements that are already reprised in the subsectors for specific modes of transport above (e.g. harbour operation), whereas others do not comply with the criteria for inclusion with respect to the proposed measures. It should be noted that for this subsector, the relevancy of companies for inclusion in the scope highly depends on the size of the company, i.e. only NIS incidents in large companies in this type of business are expected to be able to have a significant impact in terms of creating blockings or other problems in the network. Detailed data on the number of large companies for b) and c) are not available, but volumes can be estimated by taking into account the percentage of large companies in the overall subsector 'support activities for transportation'[126].

The scope of companies presented above, leads to **a total estimated number of businesses equal to ± 14 600** that are considered as relevant in the transport sector:

123 NACE Rev2 Code 52.1: operation of storage and warehouse facilities for all kinds of goods: operation of grain silos, general merchandise warehouses, refrigerated warehouses, storage tanks etc.

124 NACE Rev2 Code 52.24: loading and unloading of goods or passengers' luggage irrespective of the mode of transport used for transportation – stevedoring - loading and unloading of freight railway cars

125 NACE Rev2 Code 52.29 forwarding of freight, arranging or organising of transport operations by rail, road, sea or air, organisation of group and individual consignments (including pickup and delivery of goods and grouping of consignments), issue and procurement of transport documents and waybills, activities of customs agents, activities of sea-freight forwarders and air-cargo agents, brokerage for ship and aircraft space, goods-handling operations, e.g. temporary crating for the sole purpose of protecting the goods during transit, uncrating, sampling, weighing of goods

126 NACE Rev2 Code 52.2

	AIR TRANSPORT			RAILWAY	MARITIME TRANSPORT			AUXILARY LOGISTIC SERVICES			
	Number of commercial airports with more than 15,000 passenger unit movements per year	Number of air transport operators - passengers (commercial)	Number of air transport operators - freight	Number of railway enterprises	Number of port operators	Number of sea and coastal passenger water transport companies	Number of sea and coastal freight water transport companies	Number of large companies in warehousing and storage	Number of large companies in cargo handling	Number of large companies in other transportation support activities	Estimated total number of companies
	2009	2008	2009	2010		2009	2009	2009	2009	2009	
Belgium	5	0		1	16		74	6	3	17	122
Bulgaria	5	5	9	5	3	11	12	0	1	7	57
Czech Republic	5	0		24	0	0	1				30
Denmark	10	5	9		67	68	310	0	1	10	480
Germany	75	39	69	125	465	79	2159	46	5	198	3260
Estonia	7	0	0	9	3	20	14	0	0	2	56
Ireland	11	10	18	1							40
Greece	39	3	5	3	160	2077	741	0	0	5	3033
Spain*	42	12	22	10	16	185	72	14	4	37	414
France	63	0		1	25	370	116	19	9	68	671
Italy	43	9	16		39	466	179	6	25	47	830
Cyprus	2	0	0		0	46	2	0	1	5	57
Latvia	2	3	6	8	8	10	35	0	1	6	79
Lithuania	3	3	5	1	3	2	15	0	1	6	39
Luxembourg	1	3	6	3				1	0	1	15
Hungary	3	11	19	2	2	6	8	4	2	9	66
Malta	1	0							0	0	1
Netherlands	5	2	3	15	129	145	598	7	4	27	934
Austria	6	4	7	21	0	0	0	1	0	16	55
Poland	10	7	13	48	11	122	52	11	6	16	297
Portugal	10	4	7	5	11	132	50	1	1	8	229
Romania	9	11	19	68	20	5	95	2	2	13	244
Slovenia	3	2	4	1	4	23	17	0	1	3	57
Slovakia	6	0		16	0	0	0		1	5	28
Finland	29	1	2	1	27	127	127	2	2	10	329
Sweden	32	16	28	29	52	494	239	1	2	13	905
United Kingdom	55	169	299	40	140	565	650	52	4	53	2028
EU27	**482**	**320**	**605**	**437**	**1.200**	**5.121**	**5.600**	**173**	**77**	**581**	**14.596**

Table 3: Overview of number of actors affected in the transport market

For **air transport**, turnover information was collected through different sources, i.e. whereas for freight air transport Eurostat gives detailed turnover information per Member State that can directly be used, this is not the case for airports and passenger air transport. For these two categories, the overall indication in the abovementioned DG TREN factsheet that airlines and airports account for 135 billion EUR of business in the EU is used, i.e. it is divided by the total number of airports and passenger air transport companies (commercial airlines)[127], so as to obtain a unitary value for the average turnover of a company in these two segments of the air transport sector (168 million EUR). This unitary value can then be applied to the number of companies per Member State so as to obtain raw indications of total turnover on a country level. Finally, for traffic control, the 'Annual Analyses of the EU Air Transport Market 2010'-report[128] gives an overall figure of 8630 million EUR Gate-to-Gate Air Navigation Service (ANS) costs, which can serve as a general indication of the turnover for this sector, since providers generate their revenues from charging for en-route ANS as well as for air traffic control services at airports.

For the **railway sector**, a similar approach as for the energy sector was taken, i.e. combining information on the turnover of the sector and the number of companies in the sector[129] as available in the Eurostat structural business statistics[130], so as to have an indication of the average turnover per company (108 million EUR) that can then be applied to the number of railway operators identified above.

For the **maritime sector**, Eurostat gives detailed turnover information per Member State both for passenger and freight transport which can directly be used. Information on the turnover of ports could however not be found.

Finally, for **auxiliary logistics services**, information on the turnover for large companies is available for warehousing and storage, whereas for cargo handling and other transportation support activities this can be derived by combining the total turnover of these subsectors (all sizes of companies) with the relative importance of turnover of large companies in the overall turnover of the 'overall support activities for transportation'-class.

This leads to the following results for turnover:

127 482 airports and 320 commercial airlines

128 http://ec.europa.eu/transport/air/observatory_market/doc/annual-2010.pdf

129 See Eurostat, Structural business statistics, NACE_R1 Code I60 comprises *'Land transport; transport via pipelines'*, i.e. transport via railways, transport via pipelines and other land transport (by road or other), and is the best proxy available for estimating the average turnover of railway operators employing over 250 people.

130 Only taking into account figures for companies with more than 250 employees, due to the nature of the activities carried out by railway operators.

	AIR TRANSPORT					RAILWAY	MARITIME TRANSPORT			AUXILIARY LOGISTIC SERVICES				
	Turnover of commercial airports with more than 15,000 passenger unit movements per year	Turnover of air transport operators - passengers (commercial)	Turnover of air transport operators - freight	Turnover for air traffic control	Estimation of total turnover (Air transport)	Estimation of total turnover (Railway transport)	Turnover of sea and coastal passenger water transport companies	Turnover of sea and coastal freight water transport companies	Estimation of total turnover (Maritime transport)	Turnover of large companies in warehousing and storage	Turnover of large companies in cargo handling	Turnover of large companies in other transportation support activities	Estimation of total turnover (Auxiliary logistics)	Estimated total turnover for the transport sector
	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR	Mill EUR
Belgium	842	0			842	108		823	823	229	515	1.875	2.619	4.392
Bulgaria	842	857	25		1.724	540			0	0	19	141	159	2.423
Czech Republic	842	0			842	2.590	0		0				0	3.432
Denmark	1683	857	388		2.927	0	1174		1.174	0	35	1.759	1.795	5.896
Germany	12625	6567	2573		21.764	13.491	370	20.963	21.333	2.078	1.002	26.055	29.136	85.723
Estonia	1178	0	0		1.178	971	407		407	0		133	133	2.689
Ireland	1852	1713	82		3.646	108			0				0	3.754
Greece	6565	476	14		7.055	324	1660	448	2.108	0	56	474	530	10.017
Spain*	7070	2094	199		9.363	1.079	897	931	1.828	1.005	630	5.544	7.179	19.448
France	10605	0			10.605	108	882	9.040	9.922	4.214	1.365	16.114	21.693	42.328
Italy	7238	1523	66		8.827		5513	5.178	10.691	823	1.943	6.682	9.448	28.966
Cyprus	337	0	0		337		215		215	0	15	170	185	736
Latvia	337	571			908	863		42	42	0	148	303	451	2.264
Lithuania	505	476	40		1.021	108		147	147	0	27	138	165	1.441
Luxembourg	168	571			739	324			0		0	0	0	1.063
Hungary	505	1808	48		2.361	216	1	3	4	134	38	828	999	3.580
Malta	168	0			168				0				0	168
Netherlands	842	286			1.127	1.619		4.652	4.652	859	977	4.276	6.112	13.510
Austria	1010	666	6		1.682	2.266	0	0	0		0	0	0	3.949
Poland	1683	1237	34		2.955	5.180			0	319	240	1.049	1.608	9.743
Portugal	1683	666	19		2.369	540		349	349		0	0	0	3.257
Romania	1515	1808	18		3.341	7.339	0	64	64	23	92	353	467	11.212
Slovenia	505	381	7		893	108		50	50	0	0	0	0	1.051
Slovakia	1010	0			1.010	1.727	0	0	0		6	401	407	3.144
Finland	4882	190			5.072	108	1019	1.379	2.398		0	0	0	7.578
Sweden	5387	2665			8.051	3.130	1186	2.332	3.518		0	0	0	14.699
United Kingdom	9258	28455	1029		38.742	4.317	3352	5.413	8.765	7.281	861	7.768	15.910	67.735
EU27	**81.135**	**53.865**	**4.549**	**8.630**	**139.549**	**47.163**	**20.356**	**51.814**	**72.170**	**16.964**	**7.970**	**74.062**	**98.996**	**366.509**

Table 4: Estimation of total turnover for the transport sector[131]

131 Excluding turnover related to ports.

Financial sector

In the financial services sector, all credit institutions, irrespective of their size, are esteemed to be a possible victim of a significant security breach and this because of the nature of their activities. Unlike credit institutions, insurance companies are not considered to be relevant for inclusion in the scope of the envisaged measures. Indeed, the activities of the insurance sector are not comparable to those of credit institutions, and this for several reasons, most importantly the lesser importance of real-time availability, and also the difference in type of information dealt with.

Eurostat indicates a **total number of credit institutions of 7706** for 2007. The order of magnitude of this figure is confirmed by the European Central Bank (ECB), which indicates that there were around 8200 credit institutions in the EU at the beginning of 2011[132].

In the table at the end of this section, the number of credit institutions per Member State is further combined with the total number of persons employed in credit institutions as well as the total production value[133] of the credit institutions, so as to obtain a general indication of the average size of a credit institution.

A second category of actors relevant for inclusion in the scope of risk management measures are operators of stock exchanges. Whereas the MiFiD Directive[134] categorises the systems available for third-party buying and selling interests in financial instruments, e.g. identifying regulated markets and Multilateral Trading Facilities (MTFs), the volume of these systems, as e.g. available in the MiFiD-database[135] of the European Securities and Markets Authority (ESMA), is not an adequate basis for identifying the number of actors active on the EU market. For instance, the list of regulated markets published by the EC in 2010[136] contains more than 100 regulated markets, whereas according to the same list the number of operating entities behind these is around 55. This clearly indicates that several regulated markets are often operated by the same entity, and this observation can be extended to MTFs. The Wiener Börse AG for instance operates the regulated markets Official Market (Amtlicher Handel) and Second Regulated Market (Geregelter Freiverkehr), but also the Third Market (Wiener Börse AG Dritter Markt) as a MTF. As it can be assumed that measures for risk management will be taken at the level of the market operator, it would not be correct to make calculations at the level of the individual systems they operate. Moreover, it should be noted that European exchanges have undergone a period of consolidation, whereby several market operators are

132 82,7% of 9.921 monetary financial institutions; credit institutions are defined by the EBC as '*commercial banks, savings banks, post office banks, credit unions, etc.' (see* http://www.ecb.int/press/pr/date/2011/html/pr110114.en.html)

133 Production value measures the amount actually produced by the unit, based on sales, including changes in stocks and the resale of goods and services. The production value is defined as turnover, plus or minus the changes in stocks of finished products, work in progress and goods and services purchased for resale, minus the purchases of goods and services for resale, plus capitalised production, plus other operating income (excluding subsidies). Income and expenditure classified as financial or extra-ordinary in company accounts is excluded from production value. The production value is taken for the Eurostat Structural business statistics for NACE_R1 J6512_J6552 (i.e. monetary intermediation excl. central banking).

134 Directive 2004/39/EC on Markets in Financial Instruments

135 http://mifiddatabase.esma.europa.eu/

136 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:348:0009:0015:EN:PDF

now grouped (for instance in Euronext and OMX), which means that IT security decisions can also be expected to at least partially be centralised.

With the remarks above in mind, different lists[137] of stock exchanges in the EU were analysed, and based on these it was concluded that **the relevant number of affected actors in the EU (at a consolidated level) is expected to lie in the ranges of 25 to 30**. Turnover and other financial information on the majority of European exchanges is available in the Federation of European Securities Exchanges' (FESE) "European Exchange Report"[138].

The turnover figures associated to each of the exchanges in this report was, in the table below, allocated to the MS of incorporation or where it has its headquarters[139]. Whereas not all stock exchanges are member of FESE, this provides for a good indication of the total market size, since it covers all main actors, with the exception maybe of the London Stock Exchange (LSE), but revenue figures for this exchange were added to the table below, so as to obtain a figure as accurate as possible.

137 E.g. on www.wikinvest.com, www.world-stock-exchanges.net, en.wikipedia.org/wiki/List_of_European_stock_exchanges

138 http://www.fese.be/_lib/files/EUROPEAN_EXCHANGE_REPORT_2011_FINAL.pdf

139 Euronext turnover has thus been allocated to The Netherlands, which explains the high value for this Member State. The second largest turnover is for Germany, and the biggest part of this comes from the large exchange Deutsche Börse.

	BANKING					STOCK EXCHANGES
	Total production value for all credit institutions	Total number of persons employed in the credit institutions	Number of credit institutions	Average turnover per credit institution	Average number of persons employed per credit institution	Stock exchange revenues
	Mill EUR			Mill EUR		Mill EUR
Belgium	15.067	65.925	111	136	594	0
Bulgaria	1.605	30.189	29	55	1.041	1
Czech Republic	5.082	39.189	55	92	713	22
Denmark	12.960	47.534	158	82	301	0
Germany	129.839	679.779	1.966	66	346	2.514
Estonia	723	3.848	23	31	167	0
Ireland	0	41.865	81	0	517	21
Greece	12.327	64.720	62	199	1.044	48
Spain	61.570	275.494	357	172	772	321
France	107.961	424.732	768	141	553	0
Italy	92.350	347.029	806	115	431	0
Cyprus	2.167	11.299	214	10	53	4
Latvia	1.282	12.911	29	44	445	0
Lithuania	879	10.339	81	11	128	0
Luxembourg	:	:	:			41
Hungary	4.736	38.263	215	22	178	11
Malta		:	:			4
Netherlands	29.376	132.795	93	316	1.428	4.552
Austria	15.410	77.511	796	19	97	50
Poland	11.412	166.691	651	18	256	0
Portugal	11.762	58.769	178	66	330	0
Romania	4.318	58.300	42	103	1.388	9
Slovenia	1.127	11.647	25	45	466	2
Slovakia	1.900	21.405	26	73	823	2
Finland	6.922	25.381	358	19	71	275
Sweden	11.746	:	186	63		0
United Kingdom	179.665	504.986	396	454	1.275	1.068
EU 27	**722.186**	**3.150.601**	**7.706**	**94**	**409**	**8.944**

Table 5: Overview of turnover, employment and number of persons employed in credit institutions in the EU 27 (based on NACE_R1 codes J6512_J6552) & Overview of turnover of stock exchanges (source: FESE and LSE Annual Report 2011)

Health sector

In the health sector, relevant actors consist most importantly of hospitals providing care. Whereas trustworthy data on the number of hospitals per Member State is not readily available, based on the rule that on average there are 3 hospitals per 100 000 inhabitants[140], an estimation of the number of actors per MS, equal to **approximately 15 000**, can be made.

140 See the European Hospital and Healthcare Federation (http://www.hope.be/03activities/quality_eu-hospitals/eu_country_profiles/00-hospitals_in_europe-synthesis.pdf)

Furthermore, Eurostat provides information on the health care expenditure of a Member State per type of provider, and hospitals are considered as a specific category of providers in these statistics[141]. These health care expenditure values can be considered as equivalent to the revenues of companies in other sectors.

	Estimation of number of hospitals	Health care expenditure by provider - hospitals (2009)
		Mill EUR
Belgium	325	11.441,65
Bulgaria	227	958,91
Czech Republic	315	4.660,32
Denmark	166	11.163,55
Germany	2.452	79.186,00
Estonia	40	424,81
Ireland	134	
Greece	339	
Spain*	1.380	39.937,78
France	1.877	77.173,08
Italy	1.810	
Cyprus	24	421,99
Latvia	67	584,21
Lithuania	100	721,36
Luxembourg	15	800,19
Hungary	300	2.185,16
Malta	12	
Netherlands	497	21.505,52
Austria	251	10.920,98
Poland	1.145	7.331,46
Portugal	319	6.137,61
Romania	644	2.728,32
Slovenia	163	1.262,11
Slovakia	61	1.396,18
Finland	161	5.200,10
Sweden	280	12.819,64
United Kingdom	1.860	
EU27	**14.967**	**298.960,93**

Table 6: Overview number of hospitals[142] and total turnover[143]

Enablers of Internet services

We consider relevant those actors whose services, delivered through the Internet, are empowering key economic and social activities and which have a significant impact in case their activities are suspended for a couple of hours.

A distinction can be made between services:

141 See: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=hlth_sha_hp&lang=en

142 Based on the European Hospital and Healthcare Federation (http://www.hope.be/03activities/quality_eu-hospitals/eu_country_profiles/00-hospitals_in_europe-synthesis.pdf)

143 See Eurostat: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=hlth_sha_hp&lang=en

- *at the wholesale level*: intermediary service providers that are not visible to the end-users (i.e. back-office internet services, providing essential inputs for the provision of retail internet services)

- *at the retail level:* provided directly to end-users (businesses or citizens)

As the sector of Internet based services is evolving very quickly[144], very few statistics are available on the numbers of actors for the subsectors that would be within the scope of the obligations. The figures presented below are therefore based on sector expert opinions, sector specific company rankings, etc. They take into account that for some activities, mainly large actors are relevant (e.g. for the public cloud computing services) and for others, also smaller players can be relevant (e.g. local eCommerce platform providers). We believe they provide a good estimate of the order of magnitude of the number of actors concerned.

As for VoIP providers, abstraction was made of those that already fall within the scope of Art.13a of the Framework Directive for electronic communications. Indeed, many VoIP providers[145] can be classified as providers of publicly available electronic communications services (or of the subset of publicly available telephone services), and thus should currently already take the necessary measures to manage the risks posed to the security of their services. This is however not the case for VoIP services that offer machine-to-machine communications essentially only consisting of the provision of a product (in casu a software program), without having a genuine function in the transport of IP packets between its users. Indeed, these "*do not consist wholly or mainly in the conveyance of signals on electronic communication networks*", and are thus not considered to be an electronic communications service. These services correspond to the first of the three categories of VoIP identified in the Commission Staff Working Document on the treatment of VoIP under the EU Regulatory Framework[146]. In practice, this means that only a small part of the about 1.200 VoIP providers in the EU[147] are relevant for inclusion in the scope of the proposed measures.

The scope as defined above leads to an estimated number of actors affected today, equal to **approximately 1400:**

144 See e.g. article on the evolution of Telco activities in the cloud: http://blogs.yankeegroup.com/2012/09/20/do-telcos-have-klout-in-cloud

145 Namely those providing services where there is access to and from numbers in a national or international telephone numbering plan.

146 http://ec.europa.eu/information_society/policy/ecomm/doc/library/working_docs/406_14_voip_consult_paper_v2_1.pdf

147 Cf. http://www.voipproviderslist.com/

Category of actors	Estimated Number of actors	Some examples of actors
Actors in the wholesale market	**601**	
Public cloud computing services (*), incl. - Software as a Service (SaaS) - Platform as a Service (PaaS) - Infrastructure as a Service (IaaS) - Security as a Service (SecaaS) - Data as a Service (DaaS)	601 (**)	Main providers are large internet and IT players such as: Amazon, Salesforce, Google, Citrix, VMWare, Rackspace, Cisco, IBM, Bluelock, Joyent, Microsoft, Akamai, etc. Also telecom operators are increasingly offering public cloud services: Orange, TMobile, TelecomItalia, CenturyLink/Savvis, Level 3/Global Crossing, Verizon / Terremark, AT&T, Tata Communications/ Instacompute, etc.
Actors in the retail market	**773**	
Search engines (web search portals), incl. other services provided (e.g. Mail services, maps, etc.)	37 (***)	Google (including all services provided by Google: search, Gmail, maps, payment, voice, etc.), Yahoo (including Yahoo mail, etc.), MSN (including Bing, Hotmail, etc.), Ask, Amazon
eCommerce platform providers	470 (°)	eBAy, Booking.com, Expedia, tripadvisor, kayak.com, HomeAway, Amazon, Kapaza, immoweb, Monster, http://www.marktplaats.nl, http://www.intramarkt.be, ...
Internet payment services	5	E.g. Paypal
Cloud Services Providers (CSPs)	100	Dropbox, Apple icloud, Amazon, Picasa, Flickr, Google docs
Providers of VoIP and other communications services (incl. mobile communications platforms)	31 (°°)	Skype, Viber, WhatsApp, imessage, facetime, national VoIP operators, Research in Motion (RIM) Blackberry
Social network providers (for professionals, citizens) and blogging (°°°)	20	Facebook, Pinterest, Twitter, Linkedin, Wordpress, Over-blog, Tumblr, Foursquare, Google+, Instagram
Platforms enabling the provision and **sharing of videos**	5	Youtube, dailymotion, vimeo
Platforms enabling the **provison and sharing of music**	5	Spotify, Apple iTunes
Major on-line **computer games**	50	Sony (playstation), World of Warcraft (WoW), etc.
Application stores	50	Apple appstore, Android appstore, Amazon, Microsoft, Vodafone
Total for all relevant ICT actors	**1374**	
(*) See e.g. http://searchcloudcomputing.techtarget.com/photostory/2240149038/Top-10-cloud-providers-of-2012/1/Introduction http://www.crn.com/news/cloud/232602632/the-100-coolest-cloud-computing-vendors-of-2012.htm		
(**) Estimation based on ±500 large IT players, 20 large teleco's and on average 3 more local players per member state		
(***) Estimation based on 10 EU-wide actors and 1 additional specific local engine per country		
(°) Estimation based on 200 EU-wide platforms and on average 10 additional local platforms per country		
(°°) Estimation based on 30 communcations operators and one mobile communications platform		
(°°°) See e.g. http://en.wikipedia.org/wiki/List_of_social_networking_websites		

Table 7: Overview of number of actors affected in the ICT sector (excl. actors falling within the scope of the Telecom FWD)

For estimating the turnover related to the actors and activities presented in the table above, the best possible indication was found in the Eurostat structural business statistics on 'Information and Communication', NACE Rev2 Code 63[148]. In total, this subsector includes over 2500 companies with 20 or more persons employed:

148 NACE Rev2 Code 63: This division includes the activities of web search portals, data processing and hosting activities, as well as other activities that primarily supply information.

in mill EUR	Companies with from 20 to 49 persons employed	Companies with from 50 to 249 persons employed	Companies with 250 persons employed or more	Total (over 20 persons employed)
Turnover	6.560	11.300	18.471	36.330
Number of companies	1.648	846	173	2.667
Average turnover per company	4	13	107	

Table 8: Estimation of average company turnover (based on NACE Rev2 Code 63)

If the assumption is taken that the companies within our scope are the largest players, a global indication can be obtained of a total relevant turnover of approximately 30 billion EUR[149].

Public administrations

For the public sector, all Member State institutions at all levels (national, regional, local, etc.) have been considered within the scope of the obligations as they are all contributing to the smooth functioning of economy and society as a whole. No attempt was made however for estimating the number of individual public institutions since the objective of the cost assessment is to make a global estimate of the total cost for the public sector.

Furthermore, contrary to the other sectors, statistics for the public administration relate to the *operating costs*. Indeed, as explained in section 2, ICT spending in the public sector is typically expressed as a % of the operating expenditure instead of revenues (or 'Turnover').

The operating costs of governmental institutions are composed of intermediary consumption, compensation of employees and taxes paid on production[150]. Information on these public operating cost categories can be found in Eurostat[151] for each of the 27 EU member states. The operating costs for the general government[152] of each individual member state are presented in the table below:

149 Based on all actors with 50 persons employed or more, incl. an additional number of 400 companies with 20 people employed or more (18.471 + 11.300 + (400 * 4) = 31.370,5 million EUR

150 See Report on 'General government expenditure: Analysis by detailed economic function' (Eurostat – Statistics in focus 33/2012 - http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-12-033/EN/KS-SF-12-033-EN.PDF).

151 See Eurostat: Annual government finance statistics; Government revenue, expenditure and main aggregates (gov_a_main).

152 General government refers to all four sub-sectors of government (see 'Manual on Government Deficit and Debt, Methodologies and Working Papers, ISSN 1977-0375 - Implementation of ESA95' ; URL: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-RA-09-017/EN/KS-RA-09-017-EN.PDF):

These are:

- *central government*: this includes all administrative departments of the State and other central agencies whose competence extends normally over the whole economic territory, except for the administration of social security funds;
- *state government* : this consists of separate institutional units exercising some of the functions of government at a level below that of central government and above that of the governmental institutional units existing at local level, except for the administration of social security funds;
- *local government* : this includes those types of public administration whose competence extends to only a local part of the economic territory, apart from local agencies of social security funds;
- *social security funds* : this includes all central, state and local institutional units whose principal activity is to provide social benefits and which fulfil each of the following two criteria: (1) by law or by regulation certain

	Operating cost of the General government				
INDIC_NA	Intermediate consumption	Compensation of employees, payable	Other taxes on production, payable	Total	
	Mill EUR	Mill EUR	Mill EUR	Mill EUR	%GDP
Belgium	13.579,5	46.487,1	0,0	60.066,6	16,3
Bulgaria	2.237,4	3.420,0		5.657,4	16,3
Czech Republic	9.084,1	11.299,1	53,7	20.436,9	
Denmark	23.542,1	44.324,9	394,5	68.261,5	
Germany	127.670,0	199.820,0	70,0	327.560,0	16,3
Estonia	1.137,9	1.771,4	5,4	2.914,7	16,3
Ireland	8.582,6	18.911,9	0,0	27.494,5	
Greece	9.740,0	26.066,0	35,0	35.841,0	13,2
Spain	57.982,0	122.926,0	253,0	181.161,0	28,5
France	109.514,0	263.669,0	9.492,0	382.675,0	12,8
Italy	91.527,0	170.052,0	10.174,0	271.753,0	18,2
Cyprus	947,3	2.880,9	0,6	3.828,8	17,6
Latvia	1.418,1	1.918,5	2,5	3.339,1	16,6
Lithuania	1.731,1	3.104,5	3,1	4.838,7	16,9
Luxembourg	1.555,9	3.390,4	3,6	4.949,9	19,2
Hungary	7.582,9	10.151,1	62,6	17.796,6	17,2
Malta	419,2	870,1	0,0	1.289,3	21,5
Netherlands	46.450,0	58.866,0	676,0	105.992,0	16,7
Austria	13.015,6	28.166,5	925,9	42.108,0	15,7
Poland	21.272,6	36.159,8	368,4	57.800,8	11,5
Portugal	7.861,9	19.370,4	0,0	27.232,3	17,7
Romania	8.167,2	10.259,6	24,1	18.450,9	20,2
Slovenia	2.332,7	4.537,7	10,2	6.880,6	17,6
Slovakia	2.989,4	4.913,5	41,2	7.944,1	13,9
Finland	21.250,0	26.835,0	5,0	48.090,0	15,6
Sweden	35.513,7	54.294,3	5.082,4	94.890,4	15,9
United Kingdom	218.858,6	193.741,1	0,0	412.599,7	13,5
European Union (27 countrie	**845.962,8**	**1.368.206,7**	**27.683,2**	**2.241.852,7**	**17,7**

Table 9: Overview of operating cost of the general government (figures for 2011)

groups of the population are obliged to participate in the scheme or to pay contributions; (2) general government is responsible for the management of the institution in respect of the settlement or approval of the contributions and benefits independently from its role as supervisory body or employer.

Summary for all relevant sectors

An overview of the number of companies per sector expected to be in the scope of the proposed measures, is presented in the table below, along with the corresponding turnover figures (operating expense for public administration).

	Energy		Transport		Banking and Financial services		Health		ICT		TOTAL excl. Public administration		Public administration
	Estimated turnover of businesses within the scope of the regulation	# of businesses within scope	Estimated turnover of businesses within the scope of the regulation	# of businesses within scope	Estimated turnover of businesses within the scope of the regulation	# of businesses within scope	Estimated turnover of businesses within the scope of the regulation	# of businesses within scope	Estimated turnover of businesses within the scope of the regulation	# of businesses within scope	Estimated turnover of businesses within the scope of the regulation	# of businesses within scope	Estimated operating expense of institutions within the scope of the regulation
	Mill EUR		Mill EUR		Mill EUR		Mill EUR		Mill EUR		Mill EUR		Mill EUR
Belgium	11.506	52	4.392	122	15.067	111	11.442	325			42.407	610	60.067
Bulgaria	36.510	165	2.423	57	1.607	29	959	227			41.498	478	5.657
Czech Republic	19.472	88	3.432	30	5.104	55	4.660	315			32.668	488	20.437
Denmark	20.578	93	5.896	480	12.960	158	11.164	166			50.598	897	68.262
Germany	352.705	1.594	85.723	3.260	132.353	1.966	79.186	2.452			649.967	9.273	327.560
Estonia	15.046	68	2.689	56	723	23	425	40			18.883	187	2.915
Ireland	3.540	16	3.754	40	21	81	0	134			7.316	271	27.495
Greece	2.213	10	10.017	3.033	12.374	62	0	339			24.604	3.444	35.841
Spain	87.844	397	19.448	414	61.891	357	39.938	1.380			209.122	2.548	181.161
France	39.829	180	42.328	671	107.961	768	77.173	1.877			267.291	3.497	382.675
Italy	94.482	427	28.966	830	92.350	806	0	1.810			215.798	3.873	271.753
Cyprus	885	4	736	57	2.171	214	422	24			4.215	299	3.829
Latvia	3.540	16	2.264	79	1.282	29	584	67			7.670	191	3.339
Lithuania	4.204	19	1.441	39	879	81	721	100			7.246	239	4.839
Luxembourg	3.319	15	1.063	15			800	15			5.182	45	4.950
Hungary	5.974	27	3.580	66	4.747	215	2.185	300			16.487	608	17.797
Malta	664	3	168	1	4		0	12			837	16	1.289
Netherlands	5.532	25	13.510	934	33.928	93	21.506	497			74.474	1.550	105.992
Austria	36.952	167	3.949	55	15.460	796	10.921	251			67.281	1.269	42.108
Poland	7.523	34	9.743	297	11.412	651	7.331	1.145			36.010	2.127	57.801
Portugal	7.081	32	3.257	229	11.762	178	6.138	319			28.237	758	27.232
Romania	18.587	84	11.212	244	4.327	42	2.728	644			36.853	1.014	18.451
Slovenia	5.532	25	1.051	57	1.129	25	1.262	163			8.974	270	6.881
Slovakia	12.170	55	3.144	28	1.901	26	1.396	61			18.611	171	7.944
Finland	26.110	118	7.578	329	7.197	358	5.200	161			46.085	966	48.090
Sweden	40.935	185	14.699	905	11.746	186	12.820	280			80.200	1.556	94.890
United Kingdom	13.276	60	67.735	2.028	180.732	396	0	1.860			261.743	4.344	412.600
EU 27	**876.009**	**3.959**	**366.509**	**14.596**	**731.129**	**7.736**	**298.961**	**14.967**	**30.000**	**1.374**	**2.302.608**	**42.633**	**2.241.853**

Table 10: Estimated number of businesses expected to be in the scope of the proposed measures, incl. corresponding turnover – per sector and total operating costs of governmental institutions

STEP 2: Identification of the current underinvestment in ICT security spending

Statistics on what businesses currently are doing in terms of NIS expenditure are very scarce, not in the least because it is difficult to assess how much is spent, as security generally does not represent a separate budget line, and a number of costs might be "hidden" outside the IT budget[153]. However, Gartner[154] for instance is providing sector specific indications of the level of *actual ICT security spending* as a percentage of total IT spending in 2011. These values can further be updated for 2012 based on the indication in a recent press release by Gartner[155] that security spending in 2012 will rise with 8.4% compared to 2011.

The percentages obtained as such can be compared to the values of the businesses that are 'best in class' (and considered to be the '*Target spending'*). Best business in class is the utilities sector which has an estimated percentage of ICT security spending of 6.61% for 2012. The comparison for each sector of the current ICT security spending level with the target spending level provides an indication of *what additional ICT security spending is required.* This can first of all be expressed as a percentage of the total IT spending per sector. Combining this percentage with the sector specific global level of IT spending (as a percentage of total turnover[156]) furthermore allows to relate the *additional ICT security spending required* to the total turnover of the sectors within the scope of the Regulation.

The elements presented above lead, for each of the individual sectors within the scope of the regulation, to the following indication of additional required ICT security spending:

153 E.g. costs related to human resources, to securing buildings, higher costs paid to network suppliers that guarantee a higher security level, etc.

154 For data, see for instance "IT Key Metrics Data 2012" by Gartner, November 2011

155 http://www.gartner.com/it/page.jsp?id=2156915

156 For the public sector, this figure relate to the total operating expenditure

	Estimate of actual ICT security spending		Target spending	Additional ICT security spending required		
	ICT security spending (as % of total ICT spending)	ICT security spending (as % of total ICT spending), incl. estimated natural increase in 2012 of 8,4%	% of IT spending that should be spent on IT security spending (value for 2012)	Additional ICT security spending required (in % of total IT expenditure)	IT spending as a % of total revenue	Additional ICT security spending required (in % of total revenues)
Energy	6,1%	6,61%	6,61%	0,0%	1,10%	**0,0000%**
Transportation	2,8%	3,04%	6,61%	3,6%	3,00%	**0,1073%**
Banking and financial services	5,0%	5,42%	6,61%	1,2%	6,50%	**0,0775%**
Healthcare providers	4,0%	4,34%	6,61%	2,3%	3,30%	**0,0751%**
ICT sector (excl. telecom)	5,5%	5,96%	6,61%	0,7%	7,60%	**0,0494%**
					IT spending as a % of total operating expense	Additional ICT security spending required (in % of total operating costs)
Public sector	3,9%	4,23%	6,61%	2,4%	3,60%	**0,0859%**

Table 11: Estimation of additional ICT security spending required per sector (in % of total revenues)

Combining these percentages per sector with the total relevant turnover per sector, leads to the following total absolute costs per sector and per company:

	Additional ICT security spending required			Average turnover per company in the scope
	Per sector	Per company		Per company
	Mill EUR	EUR	in % turnover	Mill EUR
Energy	0	0,00	0,00000%	221,27
Transportation	393	26.946,51	0,10732%	25,11
Banking and financial services	567	73.250,92	0,07751%	94,51
Healthcare providers	225	15.004,83	0,07512%	19,97
ICT sector (excl. telecom)	15	10.792,66	0,04943%	21,83
TOTAL (excl. public sector)	**1.199**			
Public sector	1.925		0,08585%	
TOTAL	**3.124**			

Table 12: Estimation of additional ICT security spending required per sector (in mill EUR) and per company (in EUR)

Since energy is a utility, the methodology leads automatically to the conclusion that the energy sector is currently already sufficiently performing in terms of risk management, so no additional spending is required.

The total cost for additional ICT security spending for all of the over 42 000 businesses and the whole public sector together is estimated at **3.1 billion EUR.**

STEP 3: Assessment of the additional cost for risk management that could be caused by the Regulation on Network and information security (NIS) – Compliance cost of the NIS Regulation

In the assessment of what part of the additional costs for risk management is indeed caused by a NIS Regulation, the following two characteristics of the affected actors are of major importance:

- Some of the actors operate *critical infrastructure* (European or national);
- Many of the actors are *'data controllers'* (as defined in the Data Protection Regulation[157]).

The following table indicates in more detail to what extent each of the actors within the scope of the NIS regulation can quality for being a critical infrastructure operator or a data controller:

[157] 'Data controllers' refers to the persons or entities which collect and process personal data. For instance, a medical practitioner is usually the controller of his patients' data; a company is the controller of data on its clients and employees; a sports club is controller of its members' data and a library of its borrowers' data. Data controllers determine 'the purposes and the means of the processing of personal data'. This applies to both public and private sectors. Data controllers must respect the privacy and data protection rights of those whose personal data is entrusted to them.

Actors	Critial Infrastructure	Data controllers
Energy sector		
Generators	X	Unlikely to be data controllers
Transmission operators	X	Most will be data controllers (i.e. processing data for invoicing their customers, often citizens). Some could be data processors rather than controllers (i.e. collecting personal data that is provided to other actors for billing), but a qualification as data controller is likely to be the general rule
Distribution operator	X	
Transport sector		
Passenger transport	Some	X
Freight transport	Few	Transport companies working on behalf of other companies are most likely to be data processors in stead of controllers.
Bank sector		
Credit institutions	Possibly	X (including business banks since they process data on who is allowed to represent businesses)
Stock Exchange	X	
Health sector		
Hospitals	Probably not. eGov health care platforms probably would be, as might health insurance systems, but those would fall under public administrations below; hospitals are just users of that system	X
ICT sector		*All of these are normally data controllers, given that they rely on the creation of user profiles in almost 100% of cases. They could only deny being data controllers if they only work for businesses, and don't use profiles of any kind. That number should be fairly close to zero*
Public cloud operators		X
Search engines		X
eCommerce platforms		X
Internet Payment services	Possibly	X
Providers of VoIP and other communication services	Possibly	X
Social network providers		X
Platform for sharing videos		X
Platform for sharing music		X
On-line computer games		X
Application stores		X
Public sector		
Public administrations and institutions	Some	Most but not all will be data controllers. Exceptions could be public services that manage geographic information, monuments, public heritage, ...)

For *European* critical infrastructures, defined as critical infrastructure with cross-border relevance in transport and energy sectors) risk assessment and mitigation plans are mandatory under Directive 2008/114/EC[158]. Several MS have similar obligations for *national* critical

[158] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

infrastructure. The risk assessment and risk management plans are generally all-hazard plans, therefore including network and information security (NIS).

Furthermore, the proposal for the General Data Protection Regulation[159] obliges the controller and the processor to implement appropriate measures for the security of processing (Article 30), based on Article 17(1) of Directive 95/46/EC, extending that obligation to processors, irrespective of the contract with the controller. Articles 31 and 32 introduce an obligation to notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC.

Depending on the precise ICT security measures and requirements that will be defined for the implementation of the NIS Regulation, there could be quite some overlap with the measures already foreseen for the Critical Infrastructure (CI) operators and data controllers. *Given that there is currently no indication that there would be significant differences in the future security requirements, it can be assumed that only little additional ICT security costs*[160] *would be caused by the NIS Regulation.*

Furthermore, the extent to which additional costs could be required will also depend upon the exact *overlaps in scope*. The degree of overlaps could vary e.g. in function of the precise network and information systems that fall indeed within the scope of critical infrastructure obligations or that are handling personal data compared to all the network and information systems targeted by the NIS Regulation. Again, it is expected that the scope of the NIS Regulation will largely be overlapping with the network and information systems within the scope of CI and personal data protection measures.

Given the elements presented above, it can be assumed that an important part of the additional ICT spending required is still needed in order to fully comply with other regulations than the Network and Information Security regulation or would be made 'naturally' (i.e. because of commercial or good governance reasons) by the actors within the scope of this assessment. As such, only part of the additional cost presented in Table 13 will possibly be caused by NIS Regulation and, by consequence, be considered as a compliance cost caused by it.

The assumption that between 40% and 70% of the additional required ICT security spending will not be caused by the NIS Regulation leads to the conclusion that its compliance cost can be estimated **between approximately 1 and 2 billion EUR**. Over half of this amount (i.e. between ± 577 and 1.155 million EUR) relates to additional ICT security measures that need to be taken by the public sector.

The estimates for each individual private sector are presented in Table 14 below:

159 See COM(2012) 11 final - Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

160 If such costs would occur, they could only be measured in a later assessment of any secondary legislation introducing such standards.

	Range of additional ICT spending required, caused by NIS Regulation (Compliance cost of the NIS Regulation)					
	Per sector		Per company		in % of turnover	
	Mill EUR		EUR			
Energy	0,0	0,0	0	0	0,000%	0,000%
Transportation	118,0	236,0	8.084	16.168	0,032%	0,064%
Banking and financial services	170,0	340,0	21.975	43.951	0,023%	0,047%
Healthcare providers	67,4	134,7	4.501	9.003	0,023%	0,045%
ICT sector (excl. telecom)	4,4	8,9	3.238	6.476	0,015%	0,030%
TOTAL (excl. public sector)	**359,8**	**719,6**			in % of OPEX	
Public sector	577,4	1.154,8			0,026%	0,052%
TOTAL	**937,2**	**1.874,5**				

Table 13: Estimated compliance cost of the NIS Regulation

As regards SMEs[161] , they are the back-bone of the European economy as they constitute more than 99% of all European businesses. A considerable number of these companies are micro-enterprises, i.e. companies which employ less than 10 people and they have been excluded from the scope since they do not have the scale nor do they provide the services that would fall within the scope of the requirements.

However, there are small (up to 50 employees) and medium enterprises (from 50 to 250 employees) to which the requirements would apply.

Starting from the total compliance costs for the private sector (see Table 13), which range from 360 to 720 million EUR, the compliance cost **per small and medium enterprise** would fall in the range of **2500 and 5000 EUR**. In carrying out the calculation, it has been assumed that small and medium enterprises account for 20% of the turnover of the private companies concerned by the regulation and represent 68% of all the companies affected or just over 28,000 enterprises. This extrapolation is based on Table 2 of this Annex, which sets out the turnover (20%) and number (68%) of small and medium enterprises as opposed to the turnover and number of large enterprises in the energy sector. These values have then been applied to the other sectors concerned. The result is however to be considered as an **absolute maximum** given that for example the number of affected hospitals have been calculated on the basis of the assumption that on average there are 3 hospitals per 100 000 inhabitants and that many small credit institutions are actually part of a larger group.

[161] Micro, small and medium enterprises are defined based on the following criteria (cf.: EU recommendation 2003/361):

Company category	Employees	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

ANNEX 4: ASSESSMENT OF COSTS RELATED TO THE REQUIREMENT TO NOTIFY NIS INCIDENTS WITH A SIGNIFICANT IMPACT AND ASSOCIATED MECHANISMS/PROCESSES

Introduction

This Annex focuses on:

- Costs related to the notification of security breaches to the competent authority;
- Costs related to cooperating with the competent authority in case of specific investigations

No specific cost calculation is made for the (one-time) setting up of the necessary internal business organisation, e.g. defining internal reporting chains etc. This is because the costs associated to this setting up is considered to already be included in the costs for putting in place an adequate risk management approach. Thus, in the following only the marginal costs linked to specific recurring activities (notifying and cooperating with investigations) are considered to be additional factors to be estimated.

Unlike for the assessment of the costs linked to the implementation of NIS risk management measures, in the quantification presented below it is assumed that such costs would not differ across sectors.

Scope of the obligation

The entities that could possibly encounter (and thus need to report) a significant NIS incident would be the same as for the NIS risk management obligations.

Assumptions taken regarding salary costs

Estimates of the costs caused by regulation are often expressed by stakeholders in terms of additional time (number of hours, man/days, etc.) that is required on a yearly basis. These indications will systematically be translated into a yearly cost by using information that was collected as part of the 'Action Programme Reducing Administrative Burdens in Europe[162]. More precisely, the salary cost per MS relating to the category 'Professionals' has been taken into account. These costs are furthermore increased by 25%[163] to take into account overhead costs. This leads to an average yearly gross salary cost per FTE[164] of 60 000 EUR for the EU 27.

Costs related to the notification of security breaches to the regulatory authority

In line with the provisions currently in place in the electronic communications sector, only breaches that have a 'significant impact' would need to be notified to the competent authority. Assuming that the threshold for what constitutes a 'significant impact' would not be specified

[162] Cf. http://ec.europa.eu/enterprise/policies/smart-regulation/administrative-burdens/actionprogramme/index_en.htm#h2-6

[163] Cf. Impact Assessment Guidelines, Annex 10. page 53 http://ec.europa.eu/governance/impact/commission_guidelines/docs/ia_guidelines_annexes_en.pdf

[164] Full Time Equivalent

in detail in the legislative initiative to be adopted under Option 2, the only hypothesis that can be taken at this stage is that these thresholds would be set at a comparable level[165] as is the case currently under Art.13 a and b of the 2009 revised regulatory framework for electronic communications.

Following this, it can be assumed that the frequency of incidents, and thus of reporting, can also be extrapolated from that in the electronic communications sector. As the provisions of the Directive have only recently been implemented in several Member States (or are only in the process of implementation), there is only limited information available on the reporting that derives from the Art.13 obligations. The first ENISA annual analysis of the Art.13a incident reports[166] provides for an analysis of all significant incidents that were reported for the year 2011, and their number amounts to 51. In this report, ENISA estimates that the number of incidents that will be reported for 2012, will account for an increase by a factor of 10, i.e. **about 510 reports on significant incidents are expected for the electronic communications sector** (e.g. because many countries implemented Art.13a only late in 2011, thus not yet having received reports on significant breaches during that year).

This total yearly amount of notifications can be extrapolated to the sectors relevant for inclusion in the scope of the proposed measures. More precisely, in the electronic communications sector an average of 510 notifications is made on a total of about 12 000[167] providers (i.e. around 4%), and if this ratio is applied to the 42 633 companies identified as being in the scope of the proposed new measures[168]**, the number of additional breach notifications expected would amount to about 1700 on an annual basis.**

In line with the level of thresholds, it can also be assumed that the level/degree of detail of reporting necessary would be comparable to that under the current art. 13a, resulting in the assessment that the time needed for a business in case it would need to notify a breach, is not expected to be more than **some hours** (cf. examples of notification reports for Art. 13 in some MS). An important factor in this regard is the presumption that following a breach, no specific additional analyses or investigations would be necessary within the organisation so as to be able to report the information that is requested, which may off course not prove to be correct if implementation of the proposed measures would go far beyond what is currently applicable in the electronic communications sector. This can however not be foreseen at the moment, and further assessments would in this case need to be made at the time of contemplating imposition of such measures. Assuming a duration of 0.5 working day, **the expected cost per breach notification would be 125 EUR, leading to a total cost for notifying breaches on an annual basis of 212 500 EUR at the EU level**[169], in other words the combination of the relatively low volume of cases and limited cost per case, leads to the conclusion that the costs related to notifying breaches would be very low for the stakeholders concerned.

---

165 Whereas both for the electronic communications sector as for the sectors to which the rules would be extended, it is possible that the rules for reporting breaches to the national authority are more stringent, thus leading to a higher number of notifications, the cost linked to this is not relevant here, as it does not stem from EU but national rules.

166 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

167 General estimate based on Eurostat Information Society statistics on the number of operators and service providers for telecommunications services.

168 See Annex 2 on Assessment of costs related to the requirements to adopt a NIS Risk Management approach

169 1700 notifications *60.000EUR/12 months/20 days/2

Moreover, it is not excluded that part of this cost represents tasks that are currently already executed to comply with other requirements. Whereas for critical infrastructures, there is no reporting at the EU level foreseen[170], the same cannot be said for the proposed new data protection measures. Indeed, breaches of personal data security would need to be reported to the Data Protection Authority (DPA), and in case of incidents representing an NIS and data protection breach at the same time, it cannot be excluded that there will at least be some level of coordination that avoids duplication of activities (and costs), e.g. through establishing principles of unique breach identification. However, in view of the differences between personal data breaches and NIS breaches, it will in any case not suffice to only report in line with the rules of 1 of both types, as not all information to be provided will be similar[171], e.g. in both cases the number of persons affected are relevant, but only in case of an NIS breach will it make sense to report information on the duration of the breach. In any case, as the implementing measures are currently not yet defined, it is impossible to quantify the possible saving/economy that can be made, and this is moreover not crucial given the low overall level of costs (see previous paragraph).

Finally, it should be noted that costs could be higher in case the threshold for breaches that would actually be set by the EU for other sectors than electronic communications would imply that the number of breaches that would have to be notified would be of another order of magnitude than what is currently the case under Art. 13. However, there is currently no indication that suchlike provisions would be relevant at the EU level. Again, in case it would be considered in the future to implement these kinds of strict thresholds through delegating acts, then the costs linked to this should be analysed prior to implementation of suchlike rules.

Costs related to cooperating with the regulatory authority in case of specific investigations regarding the respect of Art 13a

As an extension of art.13b, competent authorities would be given the possibility to investigate cases of non-compliance and the effects thereof on the security of networks and information systems. Whereas it is not necessarily always the case, this opportunity is expected to mostly be taken following the notification of a breach, so that the number of breach notifications expected (1700 per year, see above) can be taken as a starting point for the number of investigations expected. More precisely, it is estimated that between 10% and 20% of this total number of notifications will lead to an in-depth investigation, corresponding to an **absolute value of 170 to 340 expected investigations per year.**

In case of an investigation, cooperation of the entity that is under investigation will be necessary. Unlike for the notification of a breach, the individual cost of such an investigation might be significant. The importance of this depends on several factors. For instance, the *methodology* decided upon by the MS to execute investigations might influence the cost and workload for the entity, e.g. would the investigation be handled internally by the competent authority, or would it oblige the business to be audited by an independent expert? Secondly, the *level of complexity* of the breach, of the sector, of the structure and specificities of the

170 See for instance the results of the benchmark presented in Annex 5

171 An overview of the ENISA proposed reporting template for Art. 13a breaches can be found in their "Annual Incident Reports 2011" (cf. above), whereas recommendations on the data to be reported in case of data breaches are identified by ENISA in "Recommendations on technical implementation guidelines of Article 4" – April 2012

business and of the root cause[172] would be influencing factors for the magnitude of investigation costs for industry. For instance, in the underlying IA of the UK on the implementation of Art. 13[173], it is supposed that an investigation would on average take about 5 months, and that the electronic communications provider would need to foresee 1 FTE for this entire period. Whereas this order of magnitude might be representative for some cases, it should be noted that the size of the businesses in the electronic communications sector that are likely to be reporting a breach, in combination with the underlying complexity of their systems and networks, would make this to be an example at the high end of the expected range of costs for an individual business in case of an investigation. Taking into account the standard salary cost defined above, **this worst case scenario would amount up to a cost for business of maximum 25 000 EUR per investigation, or 4.25 million to 8.5 million EUR[174] per year across the EU.**

172 E.g. in case of a NIS security breach, caused by a lightning, very little or no specific NIS audit would be needed for analysing what happened.

173 See "Implementing the revised EU Electronic Communications Framework – Impact Assessment" by the department for culture, media and sport, and the underlying Detica report "Impact of Security and Integrity provisions of the EU Electronic Communications Framework"

174 Assumption of an investigation costing 25.000 EUR for 10 to 20% of all NIS breach notifications.

ANNEX 5: THE SME TEST

(1) Consultation with SMEs representatives	Consultations with SMEs took place via the following process: Public consultation which ended on 15.10.2012 – this gave the opportunity to SMEs to respond. Regular bilateral meetings with specific SMEs. **Feedback from SMEs:** Individual SMEs gave a favourable opinion. They share the concerns for the rising NIS problems and the need to adopt NIS requirements in specific critical sectors such as banking, energy, transport, Internet services, public administrations.
(2) Preliminary assessment of businesses likely to be affected	See Annex 2
(3) Measurement of the impact on SMEs	Micro companies are excluded from the scope of the preferred Option. NIS compliance requirements would apply also to SMEs in all sectors covered. Starting from the compliance costs for the private sector, which range from 360 to 720 million EUR, it has been estimated that compliance costs per SME would fall in the range of 2500 and 5000 EUR.
(4) Assess alternative options and mitigating measures	For SMEs, the preferred Option would bolster a culture of risk management and would foster more effective mitigation in case of incidents. More security would hence favour the business climate and consumers' confidence. This is something that SMEs stand to benefit from. Micro companies are excluded from the scope of the preferred Option. Consequently, there is no element showing the need for SME specific measures in order to ensure compliance with the proportionality principle.

ANNEX 6: CURRENT STATE OF CAPABILITIES IN THE EU

PREPAREDNESS

National Cyber Security Strategies in the Member States

Member States are responding to the evolving threats and the multitude of actors that need to co-operate in order to respond to the threats by adopting national cyber security strategies.

National cyber security strategies must, however, not become documents without operational actions. Far from all MS that have adopted a national cyber security strategy have included a national cyber incident contingency plan in it (Czech Republic, Lithuania, Romania, Slovakia have not).

One MS (Denmark) without a national strategy has nevertheless put a national contingency plan for cyber-incidents in place.

The number of strategies still shows progress since the first stock-taking exercise initiated by the Commission at the Ministerial Conference on CIIP in Balatonfüred, when only 9 had adopted national strategies.

ENISA has in 2012 conducted an analysis of existing strategies[175] and issued an implementation guide for national cyber security strategies[176].

Competent bodies for Internet/cyber security matters in the Member States

At MS level the public sector actors involved in NIS matters include a large variety of ministries and agencies, National/Governmental CERTs, National Regulatory Authorities[177]. The responsibilities for ICT/Internet issues is spread across different Ministries depending on the topic: responsibility for NIS for businesses (most frequently in a category that spells Ministries of Economics/Industry/Enterprise/Transport/Telecommunications) for government networks (though some have it separated under the Ministry of Finance/Public Administration). A considerable number of Member States group information and network security together with national security and critical infrastructure protection under the Ministry of Interior. A handful of MS have allocated responsibility for awareness raising or fighting cyber-crime to specialised bodies and agencies. An overview identifying at national level all relevant authorities (stakeholders) and their tasks, existing policy initiatives and regulatory provisions, exchange of information between authorities and providers, national

175 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

176 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

177 For overview see ENISA Who-is-Who Directory on network and information security http://www.enisa.europa.eu/publications/who-is-who-directory-2011.

risk management processes, and preparedness and recovery measures has been done by ENISA[178].

Baseline functions for competent bodies

The baseline functions for competent bodies regulating security of networks and services in the telecom sector are:

- Enforcing compliance to the appropriate security measures that have to be taken to prevent security incidents.
- Collecting incident reports and notifying about incidents across borders and to ENISA and the Commission.

These two core functions are central in the EU-wide security legislation for the telecom sector (Article 13a of the revised telecom framework) and ENISA has developed technical guidance for the MS in implementing these functions. ENISA has set up a working group (the Article 13 a working group) of competent bodies and reached consensus about two guidelines; a guideline on incident reporting for incidents that significantly affect the continuity of electronic communications, and a guideline on minimum security measures that should guarantee the security and the integrity of the electronic communications networks and services (telephone, internet, etc.) across the EU. It is important to stress that both guidelines (described further below) have been drafted in an open discussion and consensus with the competent bodies, and that ENISA continues to work with competent bodies to elaborate this guidance and provide the necessary technical guidance to ensure that providers of electronic communications face similar technical procedures and security requirements across the EU.

Current EU-level cooperation between national bodies - EFMS

The European Forum for Member States - EFMS - was established in 2009 as a follow-up to the policy initiative on Critical Information Infrastructure Protection (CIIP) adopted by the European Commission on 30 March 2009[179]. EFMS provides a flexible, informal, responsive and continuous platform dedicated to representatives from national public authorities to foster the exchange of good practices and experiences on public policy matters relevant to CIIP. It does not address technical and operational issues. These informal discussions may complement and support formal decision-making processes (e.g. in Council Working Group).

EFMS fosters awareness and common understanding of EU challenges; stimulating discussions on common policy objectives and priorities; reinforcing collaboration between Member States and promoting a better integration of national policies in a European and global dimension. It is open to all interested officials from national competent authorities of the Member States of the European Union (EU) and **of the European Free Trade Association** (EFTA) in charge of NIS and CIIP.

178 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/policies/stock-taking-of-national-policies

179 See COM(2009)149 of 30.03.2009. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

EFMS's meeting are convened and chaired by the European Commission, DG CONNECT, with the support of ENISA, on a quarterly basis. Member States' participation to EFMS' meeting is flexible and depends on the topics under the agenda of each meeting. It is left to the discretion of Member States to decide who should attend an EFMS meeting. Twelve EFMS meetings[180] have been organised so far.

The following topics are or have been regularly discussed: (1) the definition of criteria to identify European ICT infrastructures in support to the implementation of the Directive on the Identification and Designation of European Critical Infrastructures[181], (2) the definition of priorities, principles and guidelines for Internet resilience and stability, (3) the long term strategy on the development of pan-European exercises on large scale security incidents, (4), since January 2011, International cooperation including, in particular, developments with regards the "EU-US Working Group on Cyber-security and Cyber-crime"[182], and (5), since December 2011, the European Strategy for Cyber Security.

To ensure the transparency of the process, the EFMS has been registered, in January 2011, within the Register of Commission expert group with the task to ensure "*coordination with Member States and exchange of views*"[183]. The Register indicates in particular which national competent authorities are represented at the EFMS. Rules of procedures have been adopted. ENISA has set-up a web portal with limited access for all EFMS' documents (including minutes of meetings): 133 officials from the 27 EU Member States plus Iceland, Norway and Switzerland are registered.

EFMS received strong support from Member States at the Tallinn Ministerial CIIP conference of April 2009[184] and in the Council Resolution 2009/C 321/01[185] adopted in December 2009. It is acknowledged by the MS to be an important platform for discussions and exchange of good policy practices. The UK government reply[186] to the fifth report from the House of Lords European Union Committee on the CIIP Action Plan states that the EFMS "*has been a success and has tapped into a real needed for policy makers to have an opportunity to exchange experience*".

Need for strategic and operational cooperation, coordination, early warning and mutual assistance

The increasing sophistication of threats and the global interconnectedness call for a much tighter cooperation and collaboration between Governments, as well as between public and private sectors. There is an increasing need to put in place appropriate coordination mechanisms and structures at national level, which would help ensure better cooperation and coordination at EU level amongst competent national authorities, as well as with the private

180 In June and November 2009; March, June, October 2010; January, May, September, December 2011; March, June, December 2012.
181 Council Directive 2008/114/EC
182 Established at the EU-US Summit of 20 November 2010 in Lisbon.
183 See http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2527
184 See www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf
185 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF
186 See http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/govttresponsefinal060710.pdf

sector, in cooperation with and benefiting from the support of relevant EU institutions, agencies and bodies. Cooperation needs to be established both at the technical level (CERTs), and at the strategic level (competent authorities).

Cooperation between public and private sector

Co-operation between public and private sector at MS level can contribute to a holistic national risk management process, with the aim of ensuring security of supply and network security. The approach, if applied throughout the process of risk identification, risk assessment and risk treatment, can feed into national strategies and contingency plans.

At EU level the European Public Private Partnership (EP3R) has been set-up in 2009 as a follow-up to the policy initiative on Critical Information Infrastructure Protection (CIIP).

Good practices for building Public-Private Partnerships

Public-Private Partnerships (PPPs) are essential for the Security and Resilience of Critical Information Infrastructures (CII), since a large part of them belongs to private sector stakeholders. This cooperation in the form of PPPs has evolved in many Member States depending on the environment, culture and legal framework. The need for a European view is demonstrated by the European Public Private Partnership for Resilience (EP3R) that is engaging with National PPPs and other stakeholders to address Critical Information Infrastructure Protection (CIIP) issues at European level. Recognizing the importance of such cooperation, ENISA has conducted a Study in order to collect from the experiences of existing PPPs and to identify best practices to support those countries who are establishing a well-formed partnership for the first time or are experiencing barriers and looking for an advice.

At the initial phase of the ENISA researching activity, data from both public and private stakeholders were collected across 20 countries, in order to understand the current use of co-operative models for effective Public Private Partnerships. The initial findings were presented in a Desktop Research Report[187] revealing five main components addressing the Why, Who, How, What and When questions associated when creating and maintaining PPPs. Following the Desktop Research Report, ENISA has published a Good Practice Guide[188] to help stakeholders to easily choose those aspects that will add value to their endeavours in setting up and running PPPs. The Guide identifies a list of issues which existing PPPs have addressed and the Good Practice observed in addressing these issues. To this end, 36 recommendations are included in the Guide on how to build successfully Public Private Partnerships for resilient IT security.

187 ENISA Desktop Research Report available at http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/desktop-reserach-on-public-private-partnerships

188 ENISA Good Practice Guide on Cooperative models for effective Public Private Partnerships available at http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

Despite the large number and apparent diversity, there are three main approaches taken by PPPs in addressing the problems of security and resilience of e-communication networks and systems. These have been termed:

- Prevention focused PPPs
- Response Focused PPPs
- Umbrella PPPs

The overall conclusions reached are that diversity in approach of PPPs is supported by a core set of principles and it is recognition of these common principles which paves the way for a greater cooperation between PPPs in the future.

CERT capabilities

In line with the target set by the Digital Agenda Europe flagship initiative, Member States are in the process of establishing or appointing national / governmental Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) [189].

Almost all (24) MS now have a **national/governmental CERT in place**.

Baseline capabilities for CERTs

The baseline capabilities of national/ governmental CERTs introduced by ENISA are the first attempt in defining a minimum set of capabilities that a Computer Emergency Response Team (CERT) should possess to take part and contribute to a sustainable cross-border information sharing and cooperation and are aligned with communications from the European Council and Commission that address the challenges and priorities for NIS and the critical information infrastructure protection (CIIP). These are formulated in four areas: mandate and strategy, service portfolio, operation and cooperation.

Many EU Member States (MS) have recognised the need to strengthen national cyber-security including the protection of critical information infrastructure (CII) from cyber-based and other threats. Some countries have developed national cyber-security strategies and CII protection programmes. As a rule, such strategies and programmes include requirements to reduce the vulnerability of critical networks to cyber-attacks, respond effectively when such attacks occur, and establish and maintain cooperative relationships with the national and international partners needed to operate effectively in the cyber domain. These are all areas of activity in which these teams play an important part. It is essential therefore that the activities of national / governmental CERTs (and those CERTs which by default have assumed a national / governmental role) are consistent with the objectives of such national strategies and

[189] The updated n/g CERT baseline capabilities guide is under development (ENISA WP2012/WS3/WPK3.1). It will be published at ENISA's website (www.enisa.europa.eu/act/cert) on December 2012. This updated document will further clarify the relation between n/g CERT and other national bodies (regional cooperation).

programmes and complement the structures and other arrangements in order to deliver them. This requirement has a number of implications for the mandates of CERTs.

The service portfolio of a national / governmental CERT will be determined by its mandate and its place as part of or alongside other structures responsible for delivering the national cyber-security strategy or CII protection programme. Generally speaking, however, CERT services should reduce the vulnerability of its constituency's critical networks to cyber-attacks and support effective responses to such attacks when they do occur.

The role and responsibility mandated for a national / governmental CERT and its service portfolio create particular requirements for its effective operation. One factor is that cyber-security incidents happen on a global scale, meaning that the team must be able to respond to incidents developing across international time zones. Another is that, both in dealing with its constituency and in its relationships with other CERTs, the national / governmental CERT must enjoy a reputation for contact ability and competence in order to have the credibility which underpins its operational effectiveness.

Threats to cyber-security and cyber-attacks on critical information infrastructures respect no organisational and territorial boundaries. For that reason, effective cooperation between CERTs at all levels is required to facilitate the exchange of the information and knowledge needed to reduce vulnerability and provide effective responses to cyber incidents. This includes CERTs within particular business sectors which might be affected by large-scale incidents, other CERTs within a country serving other communities, other national / governmental CERTs and internationally recognised research and development organisations. Because of the often sensitive nature of the information shared, effective cooperation of this nature requires trust and mutual respect between the bodies involved. It is thus inevitable that a national / governmental CERT must invest time and resources in building relationships with other CERTs and equivalent bodies on both a bilateral and multilateral basis. Because of the nature of threats to cyber-security and cyber incidents, there might be a need for a national / governmental CERT to develop particular relations with certain communities. These include ISPs and telecom providers because of their role in operating critical information networks, military and national security agencies that might have access to relevant threat intelligence, and law enforcement agencies where criminal activity needs to be countered. Special arrangements might be needed to facilitate sensitive relationships, such as detailed memoranda of understanding, the ability to handle classified information or agreements on the initial response to reported incidents. EU Member States may have to formulate policy on such matters where they affect legal or regulatory matters or ensure that such issues are captured at a strategic level.

ENISA is regularly updating its status reports on national / governmental CERTs and identifies shortcomings that need to be addressed in order to meet the recommendations on baseline capabilities[190].

Overview of EU level actors

[190] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

Within the EU institutions responsibilities on issues relevant to NIS are dealt with by various institutions and departments, as is the case for MS.

Within the European Commission, the *main* Directorates General involved include:

- Directorate General for Communications Networks, Content and Technology (CONNECT), former Directorate General Information Society and Media (INFSO), in charge of policy activities on NIS and on Critical Information Infrastructure Protection (CIIP), Electronic Signature Directive, eGovernment, the ICT trust and security thematic of the 7th Framework for Research and Technological Development (FP7) and the EU Regulatory Framework for Electronic Communications;

- Directorate General Home Affairs (HOME) leading policies on fighting cybercrime and on the European Programme for Critical Infrastructures Protection (EPCIP);

- Secretariat General (SG) leading activities on crisis management;

- Directorate General for Informatics (DIGIT) in charge of the IT Strategy of the European Commission and of promoting and facilitating the deployment of pan-European *e*-Government services for citizens and enterprises;

- Directorate General Human Resources and Security (HR) laying down the European Commission policy on security and hosting a Cyber Attack Response Team (CART);

- Directorate General Justice (JUST) in charge of the EU Personal Data Protection framework;

- Directorate General Enterprise and Industry (ENTR) in charge of EU industrial policy, satellite navigation, standardisation and the security thematic of FP7;

- Directorate General Internal Market (MARKT) is responsible for the Electronic Commerce Directive and for European legal frameworks in the areas of regulated professions, services, company law and corporate governance, public procurement, intellectual, industrial property and financial services;

- Directorate General Mobility and Transport (MOVE);

- Directorate General Energy (ENER);

- The European Commission Joint Research Center (JRC) provides scientific and technical support to the policy making in the area of cyber security and data protection.

The European External Action Service (EEAS) is also actively involved in international aspects related to cyber security and cybercrime.

The Inter-Service Group on cyber security/crime is coordinating and streamlining the activities of the various Commission and EEAS services in this field. It's a platform for a structured exchange on new developments with regard to cybercrime and cyber security with

the aim to improve consistency in the overall EU institutional approach towards security in cyberspace.

In the Council, the various aspects of cyber-security are discussed in different Council configurations, such as Council Working Party on Transatlantic Relations (COTRA), Council Working Party on Civil Protection (PROCIV), COTER[191], EU Military Committee (EUMC), Council Working Party on Telecommunications and Information Society (TTE) and the Political and Security Committee (PSC) / Council standing committee on internal security (COSI), Justice and Home Affairs External Working Group (JAIEX) etc. The Secretariat General of the Council (SGC) of the EU is involved in coordinating EU policy on civil protection. Its Directorate General Security, Safety and Communication and Information Systems is in charge of the security of SGC communications and information systems. In November 2012 a Friends of the Presidency Group (FoP) on Cyber Issues was set up, first as a pilot for one year, to provide a comprehensive cross-cutting forum for coordination between relevant Council configurations.

In the European Parliament, the situation is similar. Various committees (e.g. the ones for Industry, Research and Energy (ITRE), Civil Liberties, Justice and Home Affairs (LIBE), Internal Market and Consumer Protection (IMCO), Foreign Affairs (AFET)/Security and Defence (SEDE), etc.) have an interest in certain aspects of this topic. The fact that there is not a single platform for discussion on these issues was recognised as a limitation during a roundtable on Internet security which took place at the European Parliament on 30 November 2011. It was suggested to explore the possibility of setting up an (European Parliament) intergroup on cyber-issues to institutionalise the issue. It was also suggested to establish at EU level the equivalent of the US Cyber Tzar even though it is unclear to which line of responsibility this position would be reporting to.

Further to that a number of EU bodies also deal with these issues from different perspectives: the ENISA, EUROPOL, the (future) European Cybercrime Centre (EC3), the European Defence Agency (EDA).

At EU inter-institutional level, the pre-configuration team of the Computer Emergency Response Team for the EU Institutions and bodies, established in June 2011, aims at supporting the European Institutions and bodies to protect themselves against intentional and malicious attacks on their IT assets. Its scope of activities covers Announcements, Alerts and Incident Response Coordination. CERT-EU was established on a permanent basis in 2012.

The major players in the private sector are Internet Service Providers, Critical Infrastructure operators, financial institutions, the ICT industry, security companies etc.

Cyber Incident Contingency Planning

Less than half of the Member States have adopted national cyber incident contingency plans. In a cyber-environment these have a key role in defining the interdependencies between

[191] COTER brings together Member States experts from foreign affairs ministries to focus on the external aspects of terrorism.

networks in the different sectors, connected through the Internet and communications networks, and interdependencies between the different parts of the Internet architecture itself. Devising contingency plans requires good knowledge of network architectures and the contact points between sectorial networks, to identify in advance the likely repercussions of a network disruption.

The role of the contingency plan is to link together actors that need to act in a crisis situation in order to minimise the repercussions of the incident or problem. It should also outline the various possible back-up plans in case the spread of the disruption cannot be prevented.

Good practices for national contingency plans

National Contingency Plans (NCPs) are the interim structures and measures to respond and recover CII services following an incident that leads to a crisis. CIIs are the Information and Communication Technology systems, services, networks and other infrastructures which form a vital part of European economy and society. Since European society and economy are increasingly dependent on CIIs, making them more resilient to cyber crises and strengthening their security is of the utmost importance. The development of a NCP will help nations achieve these goals.

ENISA's Good Practice Guide on National Contingency Plans[192] aims to enable to develop, test, improve and maintain good and well-functioning NCP. The guide covers the elements of an NCP and its life cycle.

Elements of National Contingency Plans

A crucial part of the NCP is the definition of the cyber crisis. Though it is highly dependent on the policy of each nation it usually relates to the incident that actually or potentially exposes the confidentiality, integrity, reliability or availability of a CII with high impact. A NCP is the blueprint for responding to such a crisis, that is the plan which describes the organized and coordinated set of steps to be taken and the concrete roles and responsibilities of the crisis responders involved.

It is important to note that the national contingency plan focuses on the *national coordination* of crisis. There are many incidents in CII that occur on a daily basis and are mitigated promptly at an operational level, without necessary leading to a crisis situation.

There are four basic sections that should be included in every NCP: a) introduction, b) key definitions and activation criteria, c) structures, roles and responsibilities, and d) processes and actions.

- *Introduction*. As the first section should include the purpose and aims of the NCP, the scope, which clearly defines the parameters for contingency and the relation of the NCP with other already existing (contingency and response) plans and policies

[192] The NCPs guide is under development. It will be published at ENISA's website (www.enisa.europa.eu) on March 2012.

concerning to national crisis management in other sectors (aviation, transport, physical disasters, etc).

- *Key definitions and Activation Criteria*. This section lists and explains the criteria under which a situation occurred after an incident is considered being a crisis or not. That means when a particular situation requires the activation of this NCP in a nationally coordinated manner.

- *Structure Roles and Responsibilities*. A crisis situation related to ICT infrastructures will almost certainly involve both private and public parties and might have an international component as well, a coordinated response can only take place if every stakeholder involved knows exactly which part to play. It is important to note that the roles and responsibilities in the case of an ICT-related crisis might differ from those in other situations or crises.

- *Processes and Actions*. This section in the NCP should explain clearly what needs to be done during a (cyber) crisis:

  – coordination of the crisis response;

  – information management;

  – define a set of actions related to public affairs;

  – crisis mitigation and separate steps of detecting, analysing, responding, resolving, and terminating the crisis.

The National Contingency Plan Life Cycle

For the development and maintenance of a NCP a life cycle has to be defined. In essence a life cycle is a quality assurance and management cycle for the plans. An essential prerequisite to an effective NCP is the existence of *National Cyber Security Strategy*. By following the steps within the cycle, a nation is guided through the process of development and continuous improvement of the NCP. The steps below are guidelines for a NCP life cycle:

- understand the scenario's and threats to be prepared for;

- to design objectives, structure, roles and responsibilities of the response;

- to deploy the NCP with planning, resources and processes;

- to maintain processes and procedures;

- to test the plans underlying technology, tools and infrastructure;

- to train the people involved;

- to perform exercises and;

- to organise review and auditing;

- and improve the plan through continuous improvement.

There is scope for better alignment of national strategies through an umbrella EU strategy outlining the main, minimum features for national strategies and their common objectives.

A European Cyber Incident Contingency Plan

The CIIP Action Plan invites Member States to develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination in response to cyber incidents. A European cyber incident contingency plan building upon and interlinking with national contingency plans is to be developed by Member States with the support of ENISA by 2012. Such a plan should provide the baseline mechanisms and procedure for communications between Member States in and response to cyber incidents, risks and threats.

- A small Working Group of Member States (BE, DE, EE, ES, FR, HU, NL, PT, SE, UK) was established to develop the framework to be applied to respond to cyber crisis involving several European Member States. The group is supported by ENISA. A first draft of the European Cyber Crisis Cooperation Framework was developed and presented at the EFMS meeting of 07 March 2012. It was opened for comments and a finalised version was presented at the EFMS meeting of 12 December 2012.

EU Emergency and Crisis Coordination arrangements

- Cross-sector Crisis Coordination arrangements (CCA) were approved in 2006 and are currently under review. The current and future CCA are arrangements for political coordination at EU level supporting the Council Decision making. They do not replace sectoral mechanisms. CCA concern major emergencies or crises with a cross sectoral nature.

RESPONSE

Member States having carried out or planned national Cyber Incident exercises

At national level, 15 Member States organized their national exercises and 17 in total have plans to conduct one in the future. Looking at the 12 MS that have not carried out any exercise, 8 of them have plans to do so.

The lack of contingency plans has not prevented some MS from proceeding to cyber-incident exercises, as in the case of Greece, Hungary, Latvia, Slovakia and Spain.

Pan-European Cyber Incident exercise

All EU Member States took part in the first-ever pan-European cyber exercise Cyber Europe 2010 and the second exercise Cyber Europe 2012.

The lack of contingency plans and low number of cyber incident exercises carried out to

date is a factor for increased vulnerability of Internet infrastructure located in or operated from the EU. In particular as the cross-border elements of them are very weak.

Cooperation between National/Governmental CERTs

The 2009 CIIP Action Plan stresses that a strong European early warning and incident response capability has to rely on well-functioning National/Governmental Computer Emergency Response Teams (CERTs). To that end, the 'preparedness and prevention' pillar of the CIIP Action Plan invited Member States and concerned stakeholders to:

- Define, with the support of ENISA, a minimum level of capabilities and services for National/Governmental CERTs and incident response operations in support to pan-European cooperation.
- Make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response.

The 'detection and response' pillar of the CIIP Action Plan addresses the development and deployment of a European Information Sharing and Alert System (EISAS), reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The emphasis on citizens and Small and Medium Enterprises (SMEs) is because they constitute the largest group of Internet users in the EU. IT systems owned and operated by these users are popular victims of targeted attacks: their computers are generally less protected and they often lack expertise on NIS. In that respect, the development of well-functioning National/Governmental CERTs (Computer Emergency Response Team) and a reinforced cooperation between them is also essential to reach out to citizens and SMEs.

The Commission has financially supported two complementary projects: NEISAS (www.neisas.eu) and FISHA (www.fisha-project.eu) that have developed prototype platforms for the exchange of security related information. ENISA has produced a roadmap[193] for further development and deployment of EISAS taking stock of the results of these projects and other national initiatives. EISAS will both benefit and add value to the European network of well-functioning National/Governmental CERTs. As of 1st January 2012, the EU-funded project on Network for Information Sharing and Alerting (NISHA)[194] has started. NISHA is a follow up to the EU-funded FISHA project. The objective of NISHA is to further develop the existing prototype of the European Information Sharing and Alert System (EISAS) achieved under FISHA into a pilot version of the system.

The transnational nature of the Internet, as well as the cross-border impact of threats and disruptions, brings the need for National/governmental CERTs to cooperate and build long-term relationships, based on trust, with other CERTs and CERT communities.

Some of the most important CERT communities include:

193 http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-enhanced-roadmap-2012

194 See http://fisha-project.eu/

The European Government CERTs (EGC) group

The EGC group forms an informal association of governmental CERTs in Europe. Its members effectively co-operate on matters of incident response by building upon a fundament of mutual trust and understanding due to similarities in constituencies and problem sets.

EGC is an operational group with a technical focus. It does not determine policy, which is the responsibility of other agencies within the members' national domain. EGC members generally speak for themselves and on their own behalf.

To date, 10 EU Member States, as well as Norway and Switzerland participate in the EGC. 4 other Member States have applied for membership (Belgium, Ireland, Latvia and Luxembourg).

TF-CSIRT

TF-CSIRT is a task force that promotes collaboration between CSIRTs (Computer Security Incident Response Teams) at the European level, and liaises with similar groups in other regions.

TF-CSIRT provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment. Participants in TF-CSIRT are actively involved in establishing and operating CSIRT services in Europe and neighbouring countries.

The task force promotes the use of common standards and procedures for responding to computer security incidents. Common standards have great potential for reducing the time needed to recognise and analyse incidents, and then taking appropriate countermeasures.

The task force also assists with the establishment of new teams, and trains members of existing teams in the newest incident handling tools and techniques.

Secretarial support for this task force is provided by TERENA with funding from the GN3 project.

Whereas most of the appointed national/government CERTs participate on a voluntary basis in the **informal CERT communities FIRST and TF-CSIRT** some do not: Italy is not participating, whereas Portugal that does not have formally appointed national/government CERTs does participate. Cyprus participates as an observer and Ireland has made an application to become a member.

The weak and disparate participation in communities that could act in times of crises is a **serious shortcoming for the preparedness** against NIS attacks or technical failures with cross-border implications or requiring assistance from other MS. The voluntary nature of the communities weakens their role even further.

In order to raise the level of preparedness of national/governmental CERTs a formal network,

with clearly defined tasks and mandate, is being proposed as part of the legislative instrument. The level of confidentiality in data exchanges between national/government CERTs will have to be formally established as well.

Secure communications

STESTA[195] constitutes the European Community's own private network, isolated from the Internet and allows officials from different Ministries to communicate at a trans-European level (up to EU restricted) in a safe and prompt way.

EXCHANGE OF INFORMATION AND BEST PRACTICES

The European Strategy for Cyber Security intends to extend, through the legislative initiative which is part of it, to other sectors the obligations to ensure the appropriate management of information security risks and the notification of security breaches (extension of article 13a & 13b of e-communications Framework Directive – (FWD) 2002/21/EC amended in 2009. The lessons learned from the process of implementing the security provisions under Art.13a & 13b may feed into the discussion on the NIS legislative proposal.

However, it must be noted that the implementation process of Art.13a has not finished yet and the full picture of the challenges related to the reporting obligation under Art.13a will not be known before the results of the bottom-up approach involving the Member States and ENISA will be translated into practice.

Implementation at national level of Article 13a and 13b on security and integrity of networks and services

The extent to which the actual implementation of Article 13a and 13b has been achieved varies a lot among Member States. Several countries are facing delays in the transposition of the Regulatory Package. A few Member States have the provisions on security breach notification already in force. Most Member States indicated that they would not be ready with secondary legislation with clear instructions to their providers on Article 13a before the end of 2012 at best.

In terms of reporting network security breaches, competent NRAs have been invited to send the Commission and ENISA a summary report of the notifications received in 2011 not later than 30 April 2012 (Commission proposal made via internal COCOM working document referenced COCOM12-11[196]). The incoming reports have been summarised by ENISA in the first annual summary of incidents reported[197]

Starting from 2013, the annual summary report to the Commission and ENISA is to be submitted no later than the end of February of each calendar year, covering the notifications

[195] See http://ec.europa.eu/idabc/en/document/2097.html

[196] See http://circa.europa.eu/Public/irc/infso/cocom1/library?l=/public_2012/cocom12-11_finalpdf/_EN_1.0_&a=d

[197] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

received in the previous calendar year (from 1st January to 31 December). Competent NRAs are encouraged to use the template of the report provided in the technical guideline on reporting incidents[198] published by ENISA.

Technical guidelines on minimum security measures and reporting

Technical guideline on minimum security measures

The guideline[199] on minimum security measures describes on a high level the minimum security measures that providers of electronic communications should take to be able to comply to Article 13a, and in particular to assess the security and integrity of public electronic communication networks. The security measures in this document are categorized in different domains; Governance and risk management, Human resources security, Security of systems and facilities, Operations management, Incident management, Business continuity management, Monitoring, auditing and testing. Each domain consists of 3-4 security measures, allowing regulators to use it as a checklist for assessing compliance. These security measures have been derived from a number of leading international standards that are commonly used to ensure security and integrity. The minimum security measures provide a framework for checking the telecom providers and provide a starting point for assessing the maturity of telecom providers in countering cyber security incidents.

The guideline lists the minimum security measures NRAs should take into account when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

Good practices in the area of security breach notification (Technical Guidelines on Incident Reporting)

The technical guideline on incident reporting[200] defines how to notify other MS about cross-border incidents and how to provide ENISA and the commission with annual summary reports about the notifications received and the relevant actions taken. Although this work does not (yet) directly address how to set up national incident reporting schemes, it does provide a baseline. The good practice guide on incident reporting[201] sets the reporting in a policy and incident life-cycle context.

In particular, the guideline makes a practical interpretation and suggests thresholds for reporting to ENISA and the Commission (when an incident is 'significant') and it provides a categorization of root causes of incidents, which will allow ENISA and the Commission to assess the total impact – across the EU - of common threats, like power cuts, natural disasters or cyber-attacks. For example, the guideline specifies that an incident is significant if more

198 See http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting

199 http://www.enisa.europa.eu/act/res/reporting-incidents/minimum-security-requirements/technical-guideline-on-minimum-security-measures

200 http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting

201 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/good-practice-guide-on-incident-reporting

than 10% of citizens are affected for more than 8 hours. Based on four parameters, namely the number of users affected, duration of the incident, geographic spread and impact on emergency calls, and the thresholds set, the NRAs will report to ENISA and the EC a yearly summary of notifications received. A reporting template is also included in the guidelines to achieve harmonisation on the information gathered.

Good practices in the area of personal data breach notification

In continuation to the previous paragraph it should be noted that the two guidelines addresses only the incidents affecting security and continuity of electronic communication networks and services – personal data breach notifications are a different matter and MS, ENISA, the Article 29 working party are working to implement the data protection provisions of the updated telecom regulatory framework (Article 4 of ePrivacy Directive). Regarding data protection, ENISA published an extensive overview of the capabilities and activities of data protection authorities across the EU in 2010[202]. In 2010 only a few countries had implemented data breach notification legislation, but currently many countries are adopting data breach notification schemes, as it is part of the updated telecom regulatory package which had to be transposed in May 2011.

Extending the security breach notification to other sectors

There are [none or] very few binding national provisions for reporting security breaches in other sectors. Responsibility for resilience is quite often linked to critical infrastructure protection, or at least divided between national responsible bodies, according to sector. The same phenomenon is visible within industry, where sector-specific approaches are emerging unless a strategic approach is taken to bring industries that rely on the same technologies (e.g. SCADA systems) under the same regulatory framework.

ENISA has issued recommendations to come to terms with the shortcomings namely through a) preparedness measures, in the area of risk and vulnerability analysis and b) procedures related to the reporting of security incidents, and also to come up with clear, downstream responsibilities to different organizational units of a competent entity covering a wide-ranging set of tasks from preparation of regulation to enforcement, oversight and cooperation with the market stakeholders[203].

Member States would be free to appoint the existing competent authority under Art 13 or another appropriate body as competent authority under the legislative instrument of the European Strategy for Cyber Security.

202 http://www.enisa.europa.eu/act/it/risks-and-data-breaches/dbn

203 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations, page 30 and 100.

ANNEX 7: INTERNATIONAL ORGANISATIONS AND BODIES DEALING WITH INTERNET/CYBERSECURITY

A number of international organisations and fora deal with the issues of Internet/cybersecurity and cybercrime.

The involvement of **G8** in the field of cybercrime dates back to the late ninety, when the G8 created a mechanism to expedite contacts between countries, the so-called "G8 24/7 network of contact points". In May 2003, the G8 adopted the G8 Principles for Protecting Critical Information Infrastructures on the fight against crimes and terrorist acts committed using or against network and information systems ("cyber-crime" and "cyber-terrorism"). The G8 Justice and Home Affairs Ministers adopted in May 2004 the Best Practices for Network Security, Incident Response and Reporting to Law Enforcement and in May 2009 a significant part of the Final Declaration was devoted to cybercrime and cybersecurity, focusing on collaboration between service providers and law enforcement and on the strengthening of international cooperation.

The **OECD Working Party on Information Security and Privacy (WPISP)** is an intergovernmental forum that works under the OECD direction of the "Committee for Information, Computer and Communications Policy" (ICCP). It is supported by the OECD Secretariat within the Directorate for Science, Technology and Industry. The OECD WPISP main goal is to develop, by **consensus,** guidance and policy options to sustain trust in the Internet Economy and the global networked society in working in areas such as Critical Information Infrastructure (CII); Digital Identity Management (IDM); Cybersecurity Policies; Malware; Radio-Frequency Identification (RFID); sensor networks, privacy protection and protection of children online. OECD WPISP Participants are delegates from OECD member countries. Business, civil society, other international organisations and non-members are also sitting at the table.

The **OECD Working Party on Information Security and Privacy** develops policy options to sustain trust in the global networked society; addresses information security and privacy as complementary issues; maintains a network of experts from government, business and civil society and serves as a platform to monitor trends, share and test experiences, analyse the impact of technology on information security and privacy and develop policy guidance.

The **Organisation for Security and Cooperation in Europe (OSCE)** addresses a wide range of security-related concerns, including arms control, confidence- and security-building measures, human rights, national minorities, democratization, policing strategies, counter-terrorism and economic and environmental activities. Enhancing cyber security has become a cross-dimensional topic and endeavour in the OSCE.

Under the hospice of the **Council of Europe**, the Budapest Convention on Cybercrime was adopted on 8 November 2001 as the first international treaty addressing crimes committed using or against network and information systems (computers). It entered into force on 1 July

2004. As of April 2012, 32 countries had ratified/accesses to the Budapest Convention[204]. Still 9 EU Member States have not ratified it. It is important to note that the Budapest Convention is open for ratification/accession by States which are not members of the Council of Europe.

The **United Nations** has been the host of a number of activities related to cyber-security and cyber-crime in the past few years[205]. In 2003, through the resolution 58/32, the General Assembly requested the Secretary-General to consider threats to information security and possible cooperative measures. To this end a Group of Governmental Experts (GGE) was established in 2004 but consensus was not reached on a final report. The same theme was discussed by a "Group of Governmental Experts", appointed in 2009 in pursuance of UN General Assembly resolution 60/45 of 8 December 2005. The Group produced a report on 16 July 2010 which recommends, among other things, "*further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures*". In preparation of the 12th United Nations Congress on Crime Prevention and Criminal Justice[206] (Salvador, Brazil, 12-19 April 2010) the Secretariat of the UN Office on Drugs and Crime (UNODC) prepared a working paper in which it recommended that "*the development of a global convention against cybercrime should be given careful and favourable consideration*". While some countries where supporting such development, others strongly opposed highlighting the existence of the Budapest Convention and the need to focus on capacity-building rather than on law-making. Lastly a proposal for a UN General Assembly resolution on an International code of conduct for information security[207] was put forward by China, the Russian federation, Tajikistan and Uzbekistan in September 2011. "*The text, similar to the one tabled in past years, called on Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information. New to the draft this year, […] was a provision seeking continuation of study by a group of governmental experts to be established in 2012 of existing and potential threats in the sphere of international security and possible cooperation measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures in information science*."[208]

The **Internet Governance Forum,** which is a forum closely related to United Nations, was created in 2005. It is convened under the auspices of the Secretary-General of the UN. It was established to (among others): Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet; Discuss […] issues relating to critical Internet resources; Help to find solutions to the issues arising from the use of the Internet, of particular concern to everyday users.

---

204 See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=04/04/2012&CL=ENG

205 See an exhaustive review of the activities of the UN regarding cyber-security at http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf

206 http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress.html

207 A/66/359; http://www.fmprc.gov.cn/eng/zxxx/t858978.htm

208 See http://www.un.org/News/Press/docs/2011/gadis3442.doc.htm

The **Internet Corporation for Assigned Names and Numbers** (ICANN) is a non-profit corporation headquartered in California, United States. It was created in September 1998. ICANN coordinates the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. Besides providing technical operations of DNS resources, ICANN also defines policies for how the "names and numbers" of the Internet should run. The Security and Stability Advisory Committee (SSAC) advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

The **International Telecommunication Union** is the specialized agency of the United Nations which is responsible for Information and Communication technologies. Cybersecurity is considered in the "C5" World Summit on Information Society (WSIS) Action Line of the Geneva Action Plan on building confidence and security in the use of ICT. ITU was proposed as moderator/facilitator in implementing concrete projects and initiatives along this action. ITU deals also with adopting international standards to ensure seamless global communications and interoperability for next generation networks; building confidence and security in the use of ICTs; emergency communications to develop early warning systems and to provide access to communications during and after disasters, etc.

NATO has recently acknowledged the need to focus on cyber defence. In the 2010 Strategic Concept adopted in Lisbon, NATO Allies recognised the need for NATO to develop further the ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations. The Cooperative Cyber Defence Centre of Excellence (CCD-COE) was created in 2006. Its mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and Partners in cyber defence by virtue of education, research and development, lessons learned and consultation. The CCD-COE is located in Tallinn, Estonia.

The **London Conference on Cyberspace** (1-2 November 2011) was meant to build on the debate on developing norms of behaviour in cyberspace, as a follow-up to the speech given by UK Foreign Minister Hague at the Munich Security Conference in February 2011 which set out a number of "principles" that should underpin acceptable behaviour on cyberspace. Follow-up Conferences are planned to be hosted by Hungary (2012) and South Korea (2013).

– Forum for Incident Response and Security Teams (FIRST)

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactively as well as proactively.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Currently FIRST has more than 200 members, spread over Africa, the Americas, Asia, Europe and Oceania.

16 EU Member States are represented, out of which 11 participate with their national/governmental CERTs.

– The "Meridian Process"

The so-called "Meridian process[209]" includes annual Conferences and interim activities primarily dealing with matters related to Critical Information Infrastructure Protection (CIIP), in place since 2005. The goal of the "Meridian process" is to provide Governments worldwide with instruments for policy discussions on CIIP also enabling them to explore possibilities of cooperation with the private sector in the area.

The Meridian process began to be formalised after the first Meridian Conference in 2005, launched by the UK's NISCC (now UK Centre for the Protection of Critical Infrastructure – CPNI -) and was further strengthened after the annual Conferences that followed. The Meridian annual Conference represents the main activity under the Meridian process; since its inception in London in 2005, the Meridian Conference has been an annual forum for policy-level discussion on CIIP open to all countries and mainly designed for governmental policy makers and international organisations.

All Meridian activities represent an effort aimed at sharing experiences and best practices according to a Traffic Light Information Sharing Protocol.

Several Meridian Conferences[210] have been held in different corners of the world.

The permanent Meridian website[211] was launched after the 2007 Stockholm Conference; it is hosted by Sweden.

At the 2006 Meridian Conference in Budapest it was decided[212] (with the approval of the Meridian PC and the G8 High Tech Crime Sub-Committee) to confer the Meridian branding to the International CIIP Directory. The Directory initiative was undertaken at the G8 "CIIP Expert Conference" held in Paris in March 2003, to build upon the High Tech Crime 24x7 contact list. The Directory is maintained by the UK's Centre for the Protection for National Infrastructure[213].

Not all the EU Member States are referred to in the International CIIP Directory, nor are International organisations (such as the European Union or the United Nations).

---

209 http://meridianprocess.org/

210 See http://meridianprocess.org/Content.aspx?c=6

211 http://meridianprocess.org/

212 See page 7 of the Meridian newsletter volume 2 number 2, available at http://meridianprocess.org/library/documents/newsletter_vol1_no2.pdf

213 http://www.cpni.gov.uk/

– Standardisation organisations

Key international and regional ICT security standards development organizations are listed in part 1 of the joint ENISA, ITU and NISSG initiative on ICT security standards roadmap[214].

[214] See http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

ANNEX 8: OVERVIEW OF CURRENT REGULATORY INCENTIVES FOR NIS IN THE SECTORS CONSIDERED FOR THE EXTENSION OF ART 13 TELECOM FWD IN OPTION 4 – REGULATORY APPROACH

Introduction

The policy options assessed in the IA aim at creating a culture of risk assessment (risk management and associated measures) in sectors for which NIS are an essential input for providing their services and for the businesses with a significant impact on EU economy and society. Currently, such incentives (including enforceable notifications of breaches with a significant impact on the operation of networks and services) for risk assessment only exist for the telecom sector.

The present document aims at providing for the sectors targeted by the possible extension of the current security breach notification Directive 2009/140/EC - art. 13a&b[215] and an overview of currently existing security incentives when existing. These incentives can be either with or without a NIS dimension. They can be structured in different groups:

- Provisions regarding risk assessments and risk management
- Obligations to report NIS incidents to the competent authorities
- Sharing of information on NIS

Next to the different types of incentives, potential issues are highlighted on the identification of individual actors which will fall under the extension of the internet security breach notification. These elements will become relevant when determining the criteria for selecting those businesses to which the extension of Art. 13 would apply.

[215] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

Overview of the regulatory context regarding NIS incentives of sectors included in the extension of Article 13.

Sectors included in Extension of Article 13 (Option 3 – Regulatory option)	Current provisions regarding general risk assessment and risk management, including provisions on NIS risk assessment	Obligations to report NIS incidents	Sharing of information on NIS	Issues related to the identification of individual actors to which the incentives/obligations apply
Information society services providers – as defined by Directives 98/34/EC and 98/48/EC[216] including web certification and cloud providers	Nothing at EU level	Not at EU level	No mandatory information sharing on NIS. Business as usual[217] implies that at least large providers with an important dependence on NIS will at least participate in voluntary, informal information sharing on NIS	Players providing key inputs to important economic and societal processes (among which there are many Information society services providers) should be considered for the introduction of NIS requirements
Regulated markets whose function is underpinned by NIS[218]:				

216 Information Society service: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;"by electronic means": means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,

217 Business as usual: Common good practices in managing business imply that certain minimal standards and cooperation are assumed to be widespread since the non-compliance to these common good practices results in reputational, commercial and financial losses. Common business sense is therefore to adopt these minimal standards and coordination.

218 Cf. Sectors explicitly mentioned in the description of Option 2 – Regulatory approach

Sectors included in Extension of Article 13 (Option 3 – Regulatory option)	Current provisions regarding general risk assessment and risk management, including provisions on NIS risk assessment	Obligations to report NIS incidents	Sharing of information on NIS	Issues related to the identification of individual actors to which the incentives/obligations apply
Banking	European stress tests for systemic banks, being a risk assessment on financial stability. No direct link to NIS in these risk assessments.	Not at EU level	No mandatory information sharing on NIS. Business as usual[219] implies that banks will at least participate in voluntary, informal and specific information sharing on NIS since security breaches can lead to substantial financial losses for the bank and its customers[220].	

219 Business as usual: Common good practices in managing business imply that certain minimal standards and cooperation are assumed to be widespread since the non-compliance to these common good practices results in reputational, commercial and financial losses. Common business sense is therefore to adopt these minimal standards and coordination.

220 Risk for customers is limited by MS protective legislation. In case of financial losses due to security breaches, banks are responsible to compensate the financial losses to its customers

Sectors included in Extension of Article 13 (Option 3 – Regulatory option)	Current provisions regarding general risk assessment and risk management, including provisions on NIS risk assessment	Obligations to report NIS incidents	Sharing of information on NIS	Issues related to the identification of individual actors to which the incentives/obligations apply
Finance sector – as defined by Directive 2011/89/EU[221] **containing the banking sector, insurance sector and investment services sector**	Nothing at EU level. Since these businesses strongly depend on NIS, business as usual[222] should imply that most operators take measures already for financial and commercial reasons. However, risks might be under evaluated leading to insufficient protective measures.	Not at EU level		
Energy sector		Not at EU level Indirectly at MS level for gas, if a NIS incident leads to a disruption of gas transport, the cause of the incident must be reported to the competent authority (Regulation EU/994/2010)	Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) for private companies on a voluntary basis, which includes a workgroup on cybersecurity[223]	The regulation must avoid putting a disproportional burden on small actors since the energy sector also contains thousands of small enterprises (NACE code 40 – Energy contains 22.000 EU companies) which would be targeted by the extension of article 13a

221 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:326:0113:0141:EN:PDF – article 2 (8)

222 Business as usual: Common good practices in managing business imply that certain minimal standards and cooperation are assumed to be widespread since the non-compliance to these common good practices results in reputational, commercial and financial losses. Common business sense is therefore to adopt these minimal standards and coordination.

223 http://ec.europa.eu/energy/infrastructure/critical_en.htm

Sectors included in Extension of Article 13 (Option 3 – Regulatory option)	Current provisions regarding general risk assessment and risk management, including provisions on NIS risk assessment	Obligations to report NIS incidents	Sharing of information on NIS	Issues related to the identification of individual actors to which the incentives/obligations apply
Transport		Not at EU level		The transport sector is a very large sector with road, air, maritime, railroad and waterways. These sectors contain a large number of small actors, therefore the regulation must avoid a disproportional burden with the extension of article 13a
Operators of national critical infrastructure ***European* critical infrastructure (Directive 2008/114/EC -EPCIP) is defined as critical infrastructure with cross-border relevance in transport and energy sectors**[224] ***National* critical**	For European critical infrastructure risk assessments and mitigation, plans are mandatory under Directive 2008/114/EC. Several MS have a similar obligation for national critical infrastructure. The risk assessment and risk management plans are generally all-hazard plans,	Not at EU level. Indirectly at MS level: if a NIS incident leads to physical safety risks, thereby compromising the physical integrity of the critical infrastructure, the cause of the incident must be reported to the competent authority. NIS incidents that do not result		MS already know individual actors providers of *European* CI (EU CI) because the European critical infrastructure regulation obliged MS to identify these. There is no European regulation that obliges the MS to identify *national* critical infrastructure (NCI).which might lead to

224 Directive 2008/114/EC, annex I - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

225 http://www.crisis.ibz.be/index.php?option=com_content&task=view&id=190&Itemid=160&lang=dutch

226 http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur/bijlage1analysebeschermingvitaleinfrastructuur.pdf

Sectors included in Extension of Article 13 (Option 3 – Regulatory option)	Current provisions regarding general risk assessment and risk management, including provisions on NIS risk assessment	Obligations to report NIS incidents	Sharing of information on NIS	Issues related to the identification of individual actors to which the incentives/obligations apply
infrastructure includes all critical infrastructure in transport and energy sectors. **National authorities can further extend the scope of critical infrastructure (e.g. Belgium: financial and ICT sector[225]; Netherlands: 15 sectors- food, health, financial, ICT, transport, energy, water, chemical/nuclear, law/justice …[226])**	therefore including NIS breaches.	in compromising the physical integrity will however not automatically lead to a notification.		issues. It remains however very plausible that national authorities identify NCI based on existing national regulation. For both EC CI and NIC however, the competent authority is not necessarily the same as the competent NIS breaches authority, therefore confidentiality issues might arise, prohibiting the easy identification of relevant actors by the notification authority

Conclusions regarding the NIS incentives in sectors included in the extension of Article 13a

The conclusions regarding the NIS incentives are summarized both per type of incentive and per category of sectors. In this way a clear understanding of the impact per type of incentive and the implications on the sectors of these incentives is obtained. Per consequence, some conclusions might be partially restated in both paragraphs.

Conclusions per type of incentive

1. For a lot of sectors to which the extension would apply there are no sector wide risk assessments at EU level. Some regulated sectors have specific, national regulated, risk assessments which will not include an extensive assessment of NIS risks. For European critical infrastructure an extensive risk assessment is mandatory for all hazards, therefore including NIS risks. For national critical infrastructure, the involved sectors differ in each MS, but a similar extensive risk assessment can be expected, including NIS risks.

2. Currently, no obligations at EU level exist to notify NIS breaches in the sectors to which the extension would apply. In case of serious incidents compromising the physical integrity of critical infrastructure, the competent authorities will be informed. These incidents are however reported in detail only to the competent national authorities, not to a NIS authority and are only summarised to EU authorities in case of European critical infrastructure.

3. Sharing of information on NIS can be assumed to happen for large companies and for sectors with a high (financial) dependence on NIS. Business as usual would imply that certain minimal security standards and in-sector cooperation are assumed to be widespread, since the non-compliance to these common good practices results in reputational, commercial and financial losses. Common business sense is therefore to adopt these minimal NIS standards and participate in voluntary sector based risk coordination and communication.

4. The information society services sector and the regulated markets (banking, finance, energy and transport) all contain a large number of operators. The regulation must therefore avoid a disproportional burden on small actors in these sectors, in light of the proportionality principle. Critical infrastructures are expected to be operated by a more limited number of operators with a high risk profile, thereby reducing the risk of a disproportional burden. Issues may however arise on the confidentiality, even within MS, of the communication on NIS breaches, e.g. between different regulators or authorities.

Conclusions per category of sectors

1. Information society services providers have very limited incentives (other than reputational, commercial and financial losses in case of serious security breaches) under current legislation to perform risk assessment and to invest sufficiently in NIS measures. When imposing a new regulation on the information society services providers, attention must be made to avoid a disproportionate burden on the thousands of small eCommerce enterprises in the sector.

2. For some of the sectors within 'the regulated markets' (banking, finance, energy and transport) and in some MS the obligation to perform risk assessments and risk management already exists. This does however not, or very limited, entail an intensive assessment of NIS risks. There are also no mandatory EU NIS breach notifications. The only actual incentive is the business need to perform according to business standards, business as usual. Business as usual would imply that certain minimal security standards and in-sector cooperation are assumed to be widespread, since the non-compliance to these common good practices results in reputational, commercial and financial losses. Common business sense is therefore to adopt these minimal NIS standards and participate in voluntary sector based risk coordination and communication.

When imposing a new regulation on the regulated markets, attention must be made to avoid a disproportionate burden on the thousands of small enterprises in these regulated markets.

3. The critical infrastructure sector already has very high incentives to perform intensive risk assessments and risk management. EU legislation and presumably also the national legislation obliges the operators of (European or national) critical infrastructure to set up adequate safety measures, including reporting of NIS breaches. Notifications and information sharing could be a politically sensitive issue with regards to the national interests on security and confidentiality of their national critical infrastructures. Even within the MS, information sharing between different national authorities might prove difficult.

ANNEX 9: EU EARLY WARNING AND INCIDENT HANDLING NETWORKS IN OTHER DOMAINS THAN NIS

Scope of the benchmarking information collected

The problem statement in chapter 4 of the present report underlines the lack of mechanisms for effective cooperation and collaboration at EU level in the area of NIS. The transnational nature of the Internet, as well as the cross-border impact of threats and disruptions, brings the need for National/governmental CERTs/competent authorities to cooperate and build long-term relationships, based on trust, with other CERTs/competent authorities and CERT communities. Currently, such cooperation is limited to a number of Member States which are well-advanced in the area of NIS and which have developed the necessary mutual trust.

One of the measures to improve effective cooperation and collaboration at EU level taken in other sectors is the implementation of EU early warning and incident handling systems. The current NIS national early warning and incident handling systems differ significantly across Member States, while no EU system exists. There is a need for EU policy instruments identifying network and information security risks and vulnerabilities, setting out appropriate response mechanisms, and ensuring that these response mechanisms are known and applied by the stakeholders. The EU NIS early warning and incident handling system should support coordination among the competent authorities on cross-border network and information security risks, incidents and problems. In addition relevant information needs to be exchanged via a physical network infrastructure according to appropriate confidentiality standards.

In order to support the development of policy instruments on a EU early warning and incident handling system, a benchmark on EU early warning and incident handling systems across sectors could provide valuable information. The benchmark presented below aims at answering the following questions which are likely to be critical issues in an NIS EU early warning and response system (EU EWRS):

1. In what regulated sectors, impacted by a possible extension of the security breach notification, is there already an EU EWRS, and on what legal basis?
2. What kind of information is shared on the EU EWRS? Does this information contain confidential information? If yes, how does the system handle this confidential information?
3. Who manages the system, who contributes to information provision and who can access the information?
4. Does membership to the system imply a mandatory or a voluntary sharing of information? What are the criteria based on which the information is found mandatory to share?

To provide the necessary feedback on the goals of this benchmark a selection of sectors has been made:

- The sectors possibly impacted by the extension of the security breach notification:
  - Energy sector (gas, nuclear);
  - Financial sector (banking);

- Transport sector (maritime sector);

- Sectors where an EWRS has been operational for several years already and that are linked to public safety
  - Public health sector (communicable diseases, food and feed);
  - Civil protection sector;

- The sectors that are already impacted by the security breach notification
  - E-communications sector.

So far the information to answer the questions was found solely on desk research. Currently interviews are scheduled with the early warning network owners to complete the benchmarking analysis. The information sources are mentioned sector by sector at the end of the benchmark table in paragraph 2.

Overview of EU EWRS benchmarking info per sector

An overview of the information gathered is presented in the following table which summarises the results on the 4 main questions. From this table conclusions are drawn to support the outline of some aspects of the NIS early warning and system.

In the gas supply sector, the banking sector and the e-communications sector, no EU early warning systems are operational at this moment. There are cooperation and coordination mechanisms at EU level with regards to incident handling and policy alignment, but these mechanisms do not include a continuous information sharing network[227].

Sector	Nuclear security	Public health threats and communicable diseases	Food and feed sector	Maritime sector	Civil protection sector
Continuous EU information sharing system	Yes – European Radiological Data Exchange Platform (EURDEP)	Yes – Early Warning and Response System (EWRS) for prevention and control of diseases	Yes – Rapid Alert System for Food and Feed (RASFF)	Yes – SafeSeaNet Community vessel traffic monitoring and information system to enhance the maritime traffic safety and improve the response of authorities to incidents	Yes –Common Emergency Communication and Information System (CECIS)
Legal instrument	Council Decision 87/600/Euratom and the Recommendation 2000/473/Euratom	Commission Decision 96/2000/EC	Regulation 2002/178/EC	Directive 2002/59/EC	Council Decision 2001/792/EC, Euratom

227 Energy: http://ec.europa.eu/energy/index_en.htm
Banking: http://www.eba.europa.eu/
E-communications: http://ec.europa.eu/information_society/index_en.htm

Sector	Nuclear security	Public health threats and communicable diseases	Food and feed sector	Maritime sector	Civil protection sector
Which information is shared	Real-time environmental monitoring of radioactivity in the air, water and soil	Events of communicable diseases with (potential) relevance to more than one MS	MS notify the Commission if MS withdraws or recalls food or feed products from the market COM analyses the information (legality, completeness, classification, translation) and then forwards the incident to all the MS and to relevant third countries	- Continuous monitoring of all vessels through ship notifications: ships continuously send automatic messages on identification, course, speed, and cargo which are captured by authorities and injected in the SafeSeaNet -Port notification on arrival of ships in ports -Hazmat notification on dangerous loads -Incident reports	In the event of a major emergency within the Community, or imminent threat thereof, which causes or is capable of causing trans boundary effects or which may result in a call for assistance from one or several Member States, the Member State in which the emergency has occurred shall, without delay, notify the Commission and relevant Member States
Who is involved	The Institute for Trans uranium Elements (ITE) of the Joint Research Centre (JRC) manages the EURDEP system National authorities transmit information and can access all information	European Centre for Disease Prevention and Control (ECDC) manages the EWRS system MS Public health authorities consult the network and disseminate information	European Food Safety Authority receives the alert from the RASFF system National competent authorities transmit information to RASFF National competent authorities receive information from border	The European Maritime Safety Agency (EMSA) manages the SafeSeaNet system National Competent Authorities (SPOC for COM) transmit information and can access the information Local Competent	The European Humanitarian Aid & Civil Protection agency MIC (Monitoring and Information Centre) manages the CECIS system The MS National Contact points use the network and disseminate

Sector	Nuclear security	Public health threats and communicable diseases	Food and feed sector	Maritime sector	Civil protection sector
			control, market control, media and business/consumers	Authorities which are authorized by a national authority to access the system (e.g. port authority) - Other EU bodies and Member State institutional users can apply for membership to the network and access to the information	information
Legal obligation to share information	Mandatory	Mandatory on potential cross-border threats	Mandatory	Mandatory	Mandatory on potential cross-border threats
How is confidential information handled	-Access to real time data on EURDEP is restricted only to JRC and MS competent authorities. -Public receives similar information with a delay of 0 to 999 hours, decided per country by national authorities	-Access to EWRS is restricted only to COM and MS competent authorities	-Regulation EC/178/2002 art. 52. All information in the network is publicly available. To handle confidentiality members are not allowed to disclose information to the network which is covered by professional secrecy	- Access to SafeSeaNet is restricted to only to the EMSA, the national authorities, the local authorities and the approved users - Regulation EC/17/2009 Article 24 on Confidentiality of information: “Member States shall, in	-Access to CECIS is restricted only to the MIC and the National Contact points

Sector	Nuclear security	Public health threats and communicable diseases	Food and feed sector	Maritime sector	Civil protection sector
				accordance with Community or national legislation, take the necessary measures to ensure the confidentiality of information sent to them pursuant to this Directive, and shall only use such information in compliance with this Directive."	
Information sources	http://eurdep.jrc.ec.europa.eu/Basic/Pages/Public/Home/Default.aspx http://ec.europa.eu/energy/nuclear/safety/safety_en.htm Council Decision 87/600 Recommendation 2000/473/Euratom	https://ewrs.ecdc.europa.eu/ http://ec.europa.eu/health/index_en.htm Commission decision EC/96/2000	http://ec.europa.eu/food/food/rapidalert/index_en.htm http://ec.europa.eu/health/index_en.htm Regulation EC/178/2002	http://www.emsa.europa.eu/ http://www.emsa.europa.eu/operations/maritime-surveillance/safeseanet.html Directive 2002/59/EC amended by directive 2009/17/EC Regulation 1406/2002/EC	http://ec.europa.eu/echo/policies/disaster_response/cecis_en.htm Council decision 2001/792/EC, Euratom

Conclusions based on the benchmarking analysis

(1) In what regulated sectors, impacted by a possible extension of the security breach notification, is there already an EU EWRS, and on what legal basis?

There are already existing EU EWRS in several sectors impacted by a possible extension of the security breach notification. The maritime transport sector has an information exchange system on vessel locations and incidents. The nuclear sector, which is linked to the energy sector and to the critical infrastructure sector, has a real-time monitoring system on the dispersion of radioactivity. The banking and gas sector have no continuous, real-time, early warning system. Cooperation in these sectors is only done on a case by case basis when incidents occur.

(2) What kind of information is shared on the EU EWRS? Does this information contain confidential information? If yes, how does the system handle this confidential information?

In general, two types of information are shared on the examined EU early warning systems:

- Real-time monitoring data (environmental measures in EURDEP, vessel location in SafeSeaNet)
- Incident reports (events of communicable diseases, events of product recalls, vessel incidents, public security incidents) which might imply cross-border implications

The shared information can and does contain some degree of confidentiality in most cases. All information sharing networks take preventive measures to handle this issue. In general four types of measures are taken:

- **Restriction on the access** of the information to the competent authorities, the Commission and the operating EU Agency. This can be extended to authorised local authorities and private members;
- **Restriction on the input** of the information in the network, by only emitting information which is not considered confidential;
- **Information sharing to the public** can be an important aspect of the EWRS. To respect confidentiality, information made public contains no confidential information or the information is shared with a delay to reduce impact;
- **EU Legislation** establishing the EWRS contains an article on the obligation to respect national and EU laws on confidentiality.

(3) Who manages the system, who contributes information and who can access the information?

The system is always managed by a European agency or European authority. Within the governing board of the network, the competent national authorities are represented. This ensures a direct link to the National and European authorities and allows a better cooperation and coordination. In general, the information in the system is contributed through the competent national authority which acts as the single point of contact for the European Network. The national authority receives the information from the national information sharing network. A prerequisite for a well-functioning European network is therefore to have well-functioning national networks and a single point of contact within each Member State.

(4) Does membership to the system imply a mandatory or a voluntary sharing of information? What are the criteria based on which the information is found mandatory to share?

Membership to the system implies a mandatory sharing of information which might imply cross-border threats. All systems are based on the fact that the threats are by nature potentially cross-border, and therefore require a European approach. The sectors which have an EU EWRS are all sectors where threats (communicable diseases, food incidents, nuclear safety, and civil protection incidents) have an important cross-border dimension and which imply public health safety.

ANNEX 10: COOPERATION FRAMEWORKS ESTABLISHED AT EU LEVEL FOR PREPAREDNESS AND RESPONSE TO CROSS-BORDER THREATS IN SPECIFIC AREAS

Security of gas supply		
Legal basis and pre-existing legal framework and mechanisms	**Governance structure**	**Main obligations / Cooperation mechanisms**
Security of gas supply is a key aspect of the internal market in natural gas, implemented since Directive 98/30/EC, which already specific that security of gas supply is a "public service obligation". Legal basis: Art 194(2) TFEU (internal market for energy) for Regulation 994/2010 concerning measures to safeguard security of gas supply Ex Art. 47(2), 55 and 95 TEC for Directive 2009/73/EC concerning common rules for the internal market in natural gas	a) Competent authorities (Each MS to designate one and notify it to COM) b) COM: where appropriate, coordinates Competent authorities inter alia via Gas Coordination Group or crisis management group particularly in case of Union's emergency c) Gas Coordination Group (Composed of Competent authorities' representatives, Agency for the Cooperation of Energy Regulators, industry representative bodies). Role: facilitate coordination of measures. COM chairs and decides on composition of the Group, which shall be consulted on: – Security and emergencies – Best practises and guidelines	a) **Risk assessment**: by the given deadline, Competent authorities (after consulting private sector stakeholders) to make full assessment of the risks affecting the security of gas supply in the MS b) **Prevention Action plans** and **Emergency plans**: • Preventive Action plan and Emergency plan (compulsory): to be adopted at national level by Competent authorities after consulting private sector stakeholders, NRAs (where appropriate), other MS and COM. To be adopted by deadline, made public and notified to COM. COM, after consulting Gas Coordination Group, may recommend amendments (detailed procedure). To be updated every two years or less. • Joint Preventive action plan and joint Emergency plan at regional level (voluntary): to be adopted by Competent authorities. To be made public and notified to COM. To be updated every two years or less. Content of plans:

	– Level of security, benchmark and assessment methodologies – Testing level of preparedness – Assessment of Action plans – Coordination of measures to deal with emergencies – Assistance needed by the most affected countries d) Crisis management Group: COM can convene it in case of Union or regional emergency, relevant MS participate. e) Agency for Cooperation of Energy Regulators, Regulation 713/2009 (legal basis: former Art. 95 TEC). In specific cases, the Agency may decide upon regulatory issues of competence of Competent authorities, which may include the terms and conditions for access and operational security. e) Monitoring task force: COM, after consultation with Gas Coordination Group, shall establish permanent reserve list for this task force of industry experts and COM representatives. The Task force shall monitor and report on gas flows into the Union, in	– Roles and responsibilities of undertakings and interaction with Competent authorities – Roles and responsibilities of Competent authorities – Measures and actions to mitigate potential impact of disruptions – Designate crisis manager or team and define its role – Identify contribution of market and non-market-based measures – Mechanisms to cooperate with other Member States – List of predefined actions to make gas available in case of emergency Annex II and III of Regulation provide indicative and non-exhaustive list of market-based and non-market based measures that could be included in Preventive and Emergency action plan. c) **Union and regional emergency responses**: – Relevance at national level: Competent authorities to inform Commission – Call for assistance: Competent authority to notify COM Civil Protection monitoring and Information Centre

	cooperation with relevant third countries. f) COM Civil Protection Monitoring and Information Centre (Council Decision 2007/779/EC – legal basis Article 308 TEC): Competent authorities to give information or ask for assistance.	– Follow the plan(s) except specific cases – COM may declare Union or regional emergency: COM to convene Gas Coordination Group which will be consulted and COM to coordinate actions of Competent authorities d) **Infrastructure standard**: Each MS to ensure by given deadline that remaining infrastructure has capacity to satisfy total gas demand e) **Information exchange:** • Undertakings concerned to make available during emergencies to Competent authorities on a daily basis information on demand/supply and gas flows. • Union or regional emergency: COM may require Competent authorities to provide information on mitigation measures undertaken or planned • Follow-up of emergency: Competent authority to provide detailed assessment to COM f) **Monitoring by the Commission**: COM to carry out continuous monitoring and reporting on security of gas supply measures through annual assessment of inter alia annual reports from MS monitoring activities (Directive 2009/73/EC). g) **Regional solidarity**: (Directive 2009/73/EC): COM and other MS to be kept informed of cooperation between MS on regional or bilateral basis. The Commission may adopt Guidelines (implementing measures) for regional

		cooperation in a spirit of solidarity. h) **Safeguard measures** (Directive 2009/73/EC): In the event of a sudden crisis in the energy market or where the physical safety or security of persons, apparatus or installations or system integrity is threatened, a Member State may temporarily take the necessary safeguard measures. MS to notify other MS and COM.
Public Health Threats		
Legal basis and pre-existing legal framework and mechanisms	**Governance**	**Main obligations / cooperation mechanisms**
EU legal framework to address communicable diseases is in place since 1998. Legal basis: Ex Article 129 TEC (Public health) for Decision 2119/98/EC setting up a network for the epidemiological surveillance and control of communicable diseases in the Community Commission Decision 2000/57/EC on the EWRS Commission Decision	a) **Community network for communicable diseases:** – **Network for epidemiological surveillance**: Brings into permanent communication by technical means COM and MS authorities charged with collecting information. Procedures for dissemination of data at Community level are established. – **Early Warning and response system (EWRS) for prevention and control of diseases**: brings into permanent communications	a) **Commission Decision No 2119/98/EC**: – Defines prevention and control of communicable diseases as a range of measures, including epidemiological investigation, taken by competent public health authorities in MS to prevent and stop the spread of communicable diseases. These measures and relevant information to be forwarded by MS competent public health authorities to all other MS and COM. – MS intending to undertake measures in principle informs in advance Community network on nature and scope and consults and coordinates actions with other MS in liaison with COM. – Annex: categories of communicable diseases covered by the network (amended via Commission decision adopted following opinion of the Network committee)

2000/96/EC on communicable diseases to be progressively covered (amended by further Commission Decisions) Ex Art. 152(4) TEC - public health) for Regulation 851/2004 establishing a European Centre for disease prevention and control 2005: International Health Regulations (HIR): MS must notify the WHO public health emergencies of international concern. Art. 168(4)(c) and (5) for Proposal for a Decision on serious cross-border threats to health (COM(2011) 866)	by appropriate means COM and public health authorities in MS responsible for determining measures which may be required to protect public health. b) **COM** to provide coordination of the network in collaboration with MS. c) **Network Committee:** COM to be assisted by a Committee of MS representatives and chaired by COM to define scope of activity, nature and data and information to be collected and transmitted, guidelines on protective measures to be taken, technical means and procedures by which data are disseminated and analysed at Community level. (Commission Decision 2000/96/EC and further Decisions have been adopted following opinion of this Committee). d) **European Centre for Disease Prevention and Control** (ECDC): Mission: identify, assess and communicate current and emerging threats to human health from communicable diseases. The ECDC has taken over the epidemiological surveillance of communicable diseases and the operation of the EWRS from the Community network.	b) **Commission Decision 2000/57/EC:** – Defines events to be communicated by MS competent public health authorities to EWRS; the events listed have (also potentially) relevance to more than one MS or the whole Community. – General procedures for information exchange on those events – MS competent public health authorities to collect and exchange all necessary information on events c) **Commission Decision no 2000/96/EC:** – Lists in Annex diseases and health issues to be covered by epidemiological surveillance and the criteria for selecting them. – Community network to be put in place by modifying and integrating as appropriate existing Community-supported surveillance networks and building up new networks for diseases not yet covered by surveillance networks. d) **Commission Decision 2003/542/EC amending Decision 2000/96/EC as regards the operation of dedicated surveillance networks** – MS, through their designated structures and/or authorities, to specify a contact point for each dedicated surveillance network, delegated to be their national representative to provide data and information

	e) **Health Security Committee:** informal group of high level representatives from MS established on the basis of the Presidency Conclusions of 15 November 2001 on bioterrorism. 2011 proposal for a Decision on serious cross-border threats to health aims at formalising the Committee, as current MS involvement is voluntary and responses are not sufficiently coordinated.	– Each dedicated surveillance network to collect relevant surveillance data and information, ensure coordination within its structure and without delay communicate them to the Community network. – Dedicated surveillance network to provide the Community network with its operating procedures, addressing at least the topics listed in Annex III – Replaces Annexes addressing communicable diseases and special health issues and adds an Annex on "topics to be addressed by operating procedures of dedicated surveillance networks to be submitted to the Community network" e) **Proposal for a Decision on serious cross-border threats to health (COM(2011) 866)** – Preparedness planning: coordination of MS efforts in terms of improved preparedness and capacity building. COM to ensure coordination between national planning and between key sectors such as transport, energy and civil protection, and to support MS in setting up a joint procurement mechanism for medical countermeasures. – Information and data for risk assessment and monitoring of emerging threats: ad hoc network to be set up in situations where an MS has raised an alert on a serious threat other than a communicable disease. Communicable diseases will continue to be monitored as previously.

		– Expansion of use of the existing EWRS: to cover all serious threats to health, and not only communicable diseases. – Coordinated development of national or European public health risk assessments: for threats of biological, chemical, environmental or unknown origin in a crisis situation. – Coherent framework for the EU response to a public health crisis: formalisation of Health Security Committee to allow the EU to better coordinate national crisis responses in a public health emergency. – Common temporary public health measures: if coordination of responses is insufficient, COM may complement action of MS through adoption (via delegated act) of common temporary health measures to be implemented by MS. – Recognition of emergency situations: COM in exceptional circumstances may formally recognise the emergency by means of implementing acts that will trigger applicability of Article 2(2) Regulation No 507/2006. – International agreements: Union may conclude agreements on cooperation on cross-border threats to health covering aspects such as information sharing and collaboration on response coordination.

Financial services		
Legal basis **and pre-existing legal framework and mechanisms**	**Governance structure**	**Main obligations / Cooperation mechanisms**
Single market for financial services under development since 1976. Following financial crisis in 2007 and 2008, De Larosiere Report COM(2009) 114 "Driving European recovery" COM(2009) 252 "European financial supervision" Legal basis: Article 50, 53(1), 62 (Freedom of establishment) and 114 TFEU for Directive 2010/78/EU "Omnibus directive" Article 114 TFEU for Regulation (EU) No 1095/2010 and No 1093/2010 establishing	**a) European system of financial supervisors (ESFS), consisting of three European Supervisory Authorities** – a European Banking Authority, a European Securities and Markets Authority, and a European Insurance and Occupational Pensions Authority, Union bodies with legal personality. ESAs role is to help restore confidence; contribute to the development of a single rulebook; solve problems with cross-border firms; prevent the build-up of risks that threaten the stability of the overall financial system. ESAs were established on the basis of ECJ reasoning as in Case C-217/04 (on ENISA). b) **European Systemic Risk Board (ESRB)** established as of 1 January 2011 as an independent body with no legal personality, to monitor and assess potential threats to	a) **Supervision via network**: The three European Supervisory Authorities (ESAs) to work in a network and in tandem with the existing national supervisory authorities to safeguard financial soundness at the level of individual financial firms and protect consumers of financial services ("micro-prudential supervision"). European network to combine nationally based supervision of firms with strong coordination at European level so as to foster harmonised rules as well as coherent supervisory practice and enforcement. ESAs have the power to: – draw up specific rules for national authorities and financial institutions; – develop technical standards, guidelines and recommendations. – monitor how rules are being enforced by national supervisory authorities – take action in emergencies, including the banning of certain products; – mediate and settle disputes between national supervisors,

ESAs Article 114 TFEU for Regulation (EU) No 1092/2010 establishing a European Systemic Risk Board	financial stability that arise from macro-economic developments and from developments within the financial system as a whole ("macro-prudential supervision"). ESRB's role is to analyse information and identify risks, provide an early warning of system-wide risks and where necessary issue recommendations for remedial action. ESRB has been established on the basis of ECJ reasoning as in Case C-217/04 (on ENISA). c) **Joint Committees**: among the others, European Banking Authority (EBA) and the new European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) are required to form a Joint Committee to oversee cooperation and coordination between national supervisors in the case of financial conglomerates.	– ensure the consistent application of EU law, – where necessary, possibility of settling disagreements between national authorities, in particular in areas that require cooperation, coordination or joint decision-making by supervisory authorities from more than one MS. ESAs are able to address decisions directly to national authorities in three areas: (i) cases where they are arbitrating between national authorities both involved in the supervision of a cross-border group and where they need to agree or coordinate their position; (ii) cases where a national authority is incorrectly applying EU Regulations; (iii) in emergency situations declared by the Council. ESAs are able to take decisions directly applicable to financial institutions as a last resort in these three cases when the ESA has addressed a decision to the national supervisor and the national supervisor has not complied with it. b) **Joint Committees**: to ensure agreement and co-ordination between national supervisors of the same cross-border institution or in colleges of supervisors. c) **Direct supervision**: the European Securities and Markets Authority (ESMA) entrusted with direct supervisory powers over credit rating agencies registered in the EU and have the power to request information, to launch investigations, and to perform on-site inspections. d) **Enhancing supervision**: further prerogatives may be transferred to ESAs in

		particular in the area of financial infrastructures, with MS and EP agreement. e) **Single European rulebook**: ESAs should contribute to a common legal basis for supervisory action in the EU, by developing technical standards which could for instance determine the formats in which financial institutions have to report information to the supervisors. Differences in the national transposition of EU law stemming from exceptions, derogations, additions or ambiguities in current directives must be identified and removed, so that this core set of key standards can be defined and applied in a harmonised manner throughout the EU by all supervisors. f) **Capital requirements** (Directive 2006/48/EC): obligation of both individual credit institutions and competent authorities in supervising that "Minimum own funds requirements for operational risk" are met. 'Operational risk' means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, and includes legal risk. This could be interpreted as also including a disruption in the ICT systems.

E-communications		
Legal basis and pre-existing legal framework and mechanisms	**Governance structure**	**Main obligations / Cooperation mechanisms**
Regulated since 2002;	a) **Member States - National Regulatory**	– "National regulatory authorities" to ensure that security and

security provisions in force since 2009. Former Art. 95 TEC and Art. 114 TFEU for Framework Directive 2002/21/EC as amended by Directive 2009/140/EC	**authorities** (competent bodies designated at national level): responsibility to ensure security and integrity of public communications networks or publicly available electronic communications services b) **Undertakings** providing public communications networks or publicly available electronic communications services: responsibility to carry out c) COM: to supervise and possibility to adopt measures for implementation d) **European Network and Information Agency (ENISA)**: to provide advice and expertise e) No specific role for the **Body of European Regulators for Electronic Communications (BEREC**) which has no security prerogatives, while its mandate is to ensure consistent application of the regulatory framework.	integrity of networks are maintained, by being empowered to issue binding instructions and require undertakings to assess security, provide results of security audits, investigate cases of non-compliance. – Relevant private sector undertakings: to carry out risk assessment, adopt preventive measures, notify to competent national regulatory authorities any breaches of security or losses of integrity with a significant impact. – COM: to obtain annual summary report on notifications and actions; may adopt technical implementing measures (via regulatory procedure with scrutiny) based much as possible on European and international standards and do not prevent MS from adopting additional requirements. – (ENISA): to provide advice and expertise and promote exchange of best practises. In particular, ENISA is to obtain the annual summary report and where appropriate to obtain ad hoc notification from MS its opinion is to be taken into the utmost account by the Commission when adopting technical implementing measures. – Public/individuals: where national regulatory authorities determine that the breach is in the public interest, it may disclose it to the public.

ANNEX 11: LEGAL AND REGULATORY ASPECTS OF INFORMATION SHARING AND CROSS-BORDER COLLABORATION OF NATIONAL/GOVERNMENTAL CERTS IN EUROPE

Extract

(Study commissioned by ENISA – prepared by RAND Europe and time.lex[228])

Legal and regulatory factors for information sharing

A number of substantive legal frameworks and common horizontal issues have been identified that may positively or negatively affect the extent of cross-border information sharing. It is important to note that these factors may be seen in a positive or negative light: for example, CERTs may be more inclined to share information knowing that the peer operates under a legal framework affording the same protections to personal data. A number of legal initiatives have been taken specifically to facilitate and encourage information sharing, such as the provisions on mutual assistance requests and international cooperation in the Council of Europe's Convention on Cybercrime, or the rules with respect to cross-border exchanges of information in the Council Framework Decision on attacks against information systems. While these rules do not apply uniformly to all CERTs, they are indicative of an increased recognition at the policy level of the importance of cross-border information exchanges for information security incidents.

Nonetheless, these legal and regulatory factors can complicate the delicate balancing act that CERTs have to perform between investigating, managing and mitigating incidents and contributing to a better understanding of the relative state of cyber security, and protecting those rights and obligations provided for by certain legal and regulatory frameworks.

Clearly, the exchange of information (including in cross-border scenarios) should not be examined as a risk to certain fundamental rights (for example, privacy), without also acknowledging that these exchanges are a precondition for responding effectively to ICT incidents. Poor cyber security could undermine the exercise of other rights enshrined in the Charter of Fundamental Rights of the European Union[229] such as the protection of integrity of the person, personal life, data protection, freedom of expression and information, the freedom to conduct a business and the right to property.

Legal factors we identified as being primarily of relevance include:

- Definitions and criminal sanctions concerning different types of computer and network misuse;

[228] http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[229] The Charter of the Fundamental Rights of the European Union is a statement of fundamental political, social and economic rights granted to citizens and residents of the EU. The Charter includes such rights as the right to life, dignity, liberty and security, and the protection of private life and personal data. It became legally binding through the entry into force of the Treaty of Lisbon, on 1 December 2009

- The European legal framework governing data protection and privacy;
- Freedom of Information (FoI) and Public Sector Reuse of Information (PSI) legislation;
- Criminal procedure;
- Intellectual Property Rights;
- Confidentiality obligations;
- Determining applicable law;
- Mandate and competences of the CERT.

In addition, other legal frameworks noted include rules governing working with law enforcement, national security laws and competition law.

A number of harmonizing initiatives have aimed at reducing differences between the Member States for most of these topics, including with respect to data protection and retention, defining crimes against information systems, re-use of public sector information, and determining applicable laws. Nonetheless, as the sections below indicate, these initiatives leave a significant margin of national policy in the Member States, meaning that CERTs are still confronted with ambiguities and differences in national laws and policies. This creates uncertainty when determining if data sharing is permissible and lawful.

A commonly recurring element in this uncertainty is the variety of mandates for CERTs. Not all CERTs will have comparable mandates to intervene in any type of computer emergency. Their competences can be strongly affected by their national laws, but also by their own statutes or operating rules, depending on the legal basis of their formation (e.g. as independent entities or as part of an interior or economic affairs ministry). This also affects how they can address each of the challenges above: a national CERT with a clear legal remit defined by law may, for example, have a clearer legal basis for collecting and processing personal data relating to suspicious activities than a purely private sector CERT that oversees the security of a single communications network. Ignoring these bounds can result in evidence being tainted and/or the CERT risking its liability. Thus, for a CERT it is vitally important to have a clear mandate, and to be able to communicate this information clearly to its peers before engaging in information exchanges.

Whilst the literature review and Key Informant Interviews (KII) conducted for this study identified a number of challenging legal concerns, at the practical level not all of these concerns were noted as being of direct impact with respect to cross-border information sharing.

The research found that a degree of uncertainty remained with respect to the legal basis of much CERT cross-border coordination. Interviewees reported that CERTs' cooperation operates on an informal basis which sometimes perceives legal involvement as hampering swift and effective cooperation. CERTs participating in this study reported having

participated in cross-border information exchange. Many of the respondents to the online questionnaire indicated they had managerial or technical, rather than legal expertise.

Evidence from the research indicated that in practice, **data protection, data retention, and obligations to work with law enforcement** constituted the greatest set of challenges for cross-border CERT cooperation. The respondents to our questionnaire were most familiar with their own national legal frameworks in these areas, whereas they were less familiar with international harmonization initiatives in the same domain. For example, with respect to their own legislation 15 out of 17 respondents reported that they had at least some knowledge of definitions of computer crime or data protection and privacy law; 14 out of 17 respondents reported some knowledge of data retention rules; procedures for preserving computer data as evidence or national security rules and 13 out of 17 respondents reported at least some knowledge concerning laws about working with law enforcement.

With regard to international aspects, however, the situation is different. Here, 9 out of 17 respondents reported some understanding of international efforts to harmonies computer crime definitions (as afforded by the Convention on Cybercrime, for example). Eleven out of 17 respondents indicated some understanding of international efforts to harmonies data protection and communications privacy, whilst 9 out of 17 respondents reported some understanding of international efforts concerning national security laws.

There was least familiarity with international efforts governing rules determining the competent court, applicable law for specific incidents or legal value of evidence: only 7 out of 17 respondents indicated any degree of understanding with international harmonization regimes in this regard.

Regarding the specific legal frameworks cited as justification for their own request being denied, 12 out of 14 respondents cited data protection and privacy law as having been used as a reason to justify a declined request by a peer. On the other hand, 5 out of 13 respondents indicated that with some degree of frequency data protection and privacy laws; rules concerning computer data as evidence; laws concerning cross-border mutual legal assistance; laws concerning working with law enforcement or rules concerning the legal value of evidence were all cited as a justification to withhold information in a cross-border request. Of course, this should not be taken as clear proof that such exchanges would certainly have been in clear breach of these laws, but rather that sufficient doubt existed on the legality of the exchanges to withhold them.

Recommendations

The evidence gathered during our study (especially from the online questionnaire) should not be taken as entirely representative of the entirety of the European national/governmental CERT community. Nonetheless, below we identify some recommendations which may further improve the work of CERTs based on the material gathered during this study. We split these up into short, medium and long-term recommendations. In the short term:

- **A.1 Identify ways to support operational coordination between CERTs** – for example by the provision of a one stop shop or legal helpline, modeled perhaps on the

European Judicial Network (EJN) 'legal helpdesk'. Other approaches include the provision of checklists.

- **A.2 Disseminate Declared Level of Service templates** building upon the establishment of common 'declared level of service' templates (based on the RFC23508 model) to help set expectations as to legal factors which may affect cross-border information exchange;

- **A.3 Investigate measures to encourage cross-border information exchange** for example via sanitization of data, confidentiality charters or means to limit liability of CERT incident response activities (such as the 2011 Danish law concerning Incident Response).

Over the medium to longer term, more extensive recommendations concern policy intervention:

- B1. Address legal uncertainty concerning requests via clarification of the differences between relevant national legal frameworks to remove uncertainty and create a common baseline for cooperation.

- B.2 Designate national/governmental CERTs on a specific regulatory basis to provide them with a clearer mandate.

- B.3 Ensure EU-level legislation takes account of the scope of national/governmental CERTs particularly with the current revision of the Data Protection Directive 95/46/EC noting principles for the use of personal data in the fight against terrorism and serious and organised crime.

- B.4 Specify a threshold for incidents requiring national/governmental CERT response and sharing – that incidents must pass some certain threshold according to agreed indicators for them to be considered as within the competence of being addressed by a national/governmental CERT.

- B.5 Articulate why CERTs need to process personal data to the relevant authorities so that guidance may be prepared to establish clarity on under what circumstances personal data used by CERTs may be shared across borders.

Finally, three long-term recommendations concern research activities or projects.

- **C.1 Incorporate information on the legal basis for an information request** (e.g. via coordination with structured information exchange initiatives such as those run by the IETF or ITU).

- **C.2 Further foster R&D into privacy enhancing Security Event & Incident Monitoring (SEIM) tools**, for example anonymisation infrastructure.

- **C.3 Conduct further empirical research into the mechanics of cross-border CERT cooperation** to explore the logic and process of cross-border incident response.

ANNEX 12: INTERNET 2011 IN NUMBERS

Source: http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/

Email

- **3.146 billion –** Number of email accounts worldwide.
- **27.6% – Microsoft Outlook was the most popular email client.**
- **19% – Percentage of spam emails delivered to corporate email inboxes despite spam filters.**
- **112 – Number of emails sent and received per day by the average corporate user.**
- **71% – Percentage of worldwide email traffic that was spam (November 2011).**
- **360 million – Total number of Hotmail users (largest email service in the world).**
- **$44.25 – The estimated return on $1 invested in email marketing in 2011.**
- **40 – Years since the first email was sent, in 1971.**
- **0.39% – Percentage of email that was malicious (November 2011).**
- **Websites**
- **555 million – Number of websites (December 2011).**
- **300 million – Added websites in 2011.**

Web servers

- **239.1% – Growth in the number of Apache websites in 2011.**
- **68.7% – Growth in the number of IIS websites in 2011.**
- **34.4% – Growth in the number of NGINX websites in 2011.**

- **80.9% – Growth in the number of Google websites in 2011.**

- **Domain names**

- **95.5 million – Number of .com domain names at the end of 2011.**

- **13.8 million – Number of .net domain names at the end of 2011.**

- **9.3 million – Number of .org domains names at the end of 2011.**

- **7.6 million – Number of .info domain names at the end of 2011.**

- **2.1 million – Number of .biz domain names at the end of 2011.**

- **220 million – Number of registered domain names (Q3, 2011).**

- **86.9 million – Number of country code top-level domains (.CN, .UK, .DE, etc.) (Q3, 2011).**

- **324 – Number of top-level domains.**

- **28% – Market share for BIND, the number one DNS server type.**

- **$2.6 million – The price for social.com, the most expensive domain name sold in 2011.**

Internet users

- **2.1 billion – Internet users worldwide.**

- **922.2 million – Internet users in Asia.**

- **476.2 million – Internet users in Europe.**

- **271.1 million – Internet users in North America.**

- **215.9 million – Internet users in Latin America / Caribbean.**

- **118.6 million – Internet users in Africa.**

- **68.6 million – Internet users in the Middle East.**

- **21.3 million – Internet users in Oceania / Australia.**
- **45% – Share of Internet users under the age of 25.**
- **485 million – Number of Internet users in China, more than any other country in the world.**
- **36.3% – Internet penetration in China.**
- **591 million – Number of fixed (wired) broadband subscriptions worldwide.**

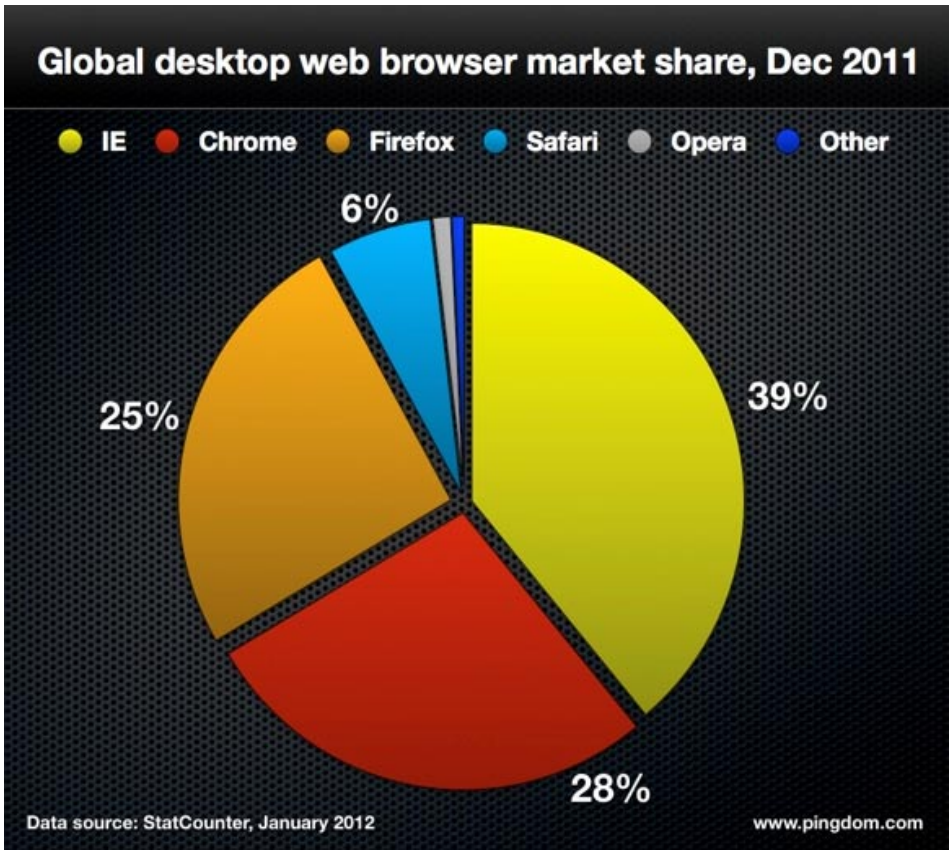
Social media

- **800+ million – Number of users on Facebook by the end of 2011.**
- **200 million – Number of users added to Facebook during 2011.**
- **350 million – Number of Facebook users that log in to the service using their mobile phone.**
- **225 million – Number of Twitter accounts.**
- **100 million – Number of active Twitter users in 2011.**
- **18.1 million – People following Lady Gaga. Twitter's most popular user.**
- **250 million – Number of tweets per day (October 2011).**
- **1 – #egypt was the number one hashtag on Twitter.**
- **8,868 – Number of tweets per second in August for the MTV Video Music Awards.**
- **$50,000 – The amount raised for charity by the most retweeted tweet of 2011.**
- **39 million – The number of Tumblr blogs by the end of 2011.**
- **70 million – Total number of WordPress blogs by the end of 2011.**
- **1 billion – The number of messages sent with WhatsApp during one day (October 2011).**

- **2.6 billion – Worldwide IM accounts.**

- **2.4 billion – Social networking accounts worldwide.**

Web browsers



Mobile

- **1.2 billion – The number of active mobile broadband subscriptions worldwide in 2011.**

- **5.9 billion – The estimated number of mobile subscriptions worldwide in 2011.**

- **85% – Percentage of handsets shipped globally in 2011 that included a web browser.**

- **88% – Apple iPad's share of global tablet web traffic in December.**

Videos

- **1 trillion – The number of video playbacks on YouTube.**

- **140 – The number of YouTube video playbacks per person on Earth.**

- **48 hours – The amount of video uploaded to YouTube every minute.**

- **1 – The most viewed video on YouTube during 2011 was Rebecka Black's "Friday."**
- **82.5% – Percentage of the U.S. Internet audience that viewed video online.**
- **76.4% – YouTube's share of the U.S. video website market (December 2011).**
- **4,189,214 – Number of new users on Vimeo.**
- **201.4 billion – Number of videos viewed online per month (October 2011).**
- **88.3 billion – Videos viewed per month on Google sites, incl. YouTube (October 2011).**
- **43% – Share of all worldwide video views delivered by Google sites, incl. YouTube.**

Images

- **14 million – Number of Instagram accounts created during 2011.**
- **60 – The average number of photos uploaded per second to Instagram.**
- **100 billion – Estimated number of photos on Facebook by mid-2011.**
- **51 million – Total number of registered users on Flickr.**
- **4.5 million – Number of photos uploaded to Flickr each day.**
- **6 billion – Photos hosted on Flickr (August 2011).**
- **1 – Apple iPhone 4 is the most popular camera on Flickr.**

ANNEX 13: IMPACT ASSESSMENT MATRIX

The matrix presents the determination of the expected impacts per policy option.

The assessment of the impacts under each of the options was done by analysing the *magnitude* of the expected impact, as well as the *likelihood* that the impact will actually occur as a result of the proposed policy option.

The notation used to express the magnitude of an impact in comparison with to baseline scenario is the following:

- - - very negative impact - 3

- - negative impact - 2

- slightly negative impact - 1

0 no impact 0

+ slightly positive impact + 1

+ + positive impact + 2

+ + + very positive impact + 3

The likelihood will be expressed as follows:

1 low likelihood 1

2 medium likelihood 2

3 high likelihood 3

The magnitude of the impact is weighed by to likelihood. The value given for the likelihood is an absolute score, i.e. not relative to the score of the baseline scenario.

Impacts	Option 1 Business as usual				Option Regulatory approach
Objective 1: To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness and response					
	Magnitude		**Likelihood**		**Magnitude (compared to baseline**
To ensure that all the Member States are adequately equipped at national level both in terms of technical and organisational capabilities to prevent, detect, mitigate and respond to NIS risks, threats and incidents	Given that initiatives would be voluntary in nature, the pace of development would vary significantly across the MS. Whereas in those MS which already consider NIS as a priority the level of security might further improve, the other Member States will continue to lag behind. The overall level of security would not improve adequately and in a timely fashion.	0	High	3	The obligations on the Member S should in principle ensure a com minimum high level of capabi across the EU. As a result, the lev security should improve considerab
To ensure that all Member States develop and update national cyber security strategies and national cyber incident contingency/cooperation plan	Given that initiatives would be voluntary in nature, the pace of development would vary significantly across the MS. Whereas in those MS which already consider NIS as a priority the level of security might further improve, the other Member States will continue to lag behind. The overall level of security would not improve adequately and in a timely	0	High	3	The obligations on the Member S should in principle ensure a com minimum high level of capabi across the EU. As a result, the lev security should improve considerab

	fashion.				
Total score Objective 1		***0***			
Objective 2: To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively					
	Magnitude		**Likelihood**		**Magnitude (compared to baseline**
To ensure that national competent authorities and CERTs share NIS information and best practices regularly	On the basis of voluntary initiatives and in the absence of a minimum level of capabilities in the Member States there would be no development of trust across the EU and there would be no guarantee that cooperation involving all the Member States would take place. Existing mechanisms involving would continue to involve only few Member States.	0	High	3	A common minimum level preparedness at national level w contribute to the creation of a clima mutual trust, thereby enabling c cooperation and allowing coherent coordinated prevention and respons cross-border NIS incidents, risks threats.

To make sure that national competent authorities and CERTs can exchange information cross-border in a reliable and confidential manner	Current mechanisms lack a framework and an infrastructure for trusted information sharing, based on common confidentiality requirements. This would hinder information exchange on NIS threats and incidents across the Member States.	0	High	3	Competent authorities coopera within the network would provide effective cross-border exchange information on NIS threats incidents. A secure infrastructure w guarantee the necessary confidentia
Total score: Objective 2		***0***			
Objective 3: To create a culture of risk management and improve the sharing of information between the private and public sectors					
	Magnitude (compared to baseline)		**Likelihood**		**Magnitude**
To make sure that key private sector players and public administrations engage in assessment of the risks and risk management practises	Only electronic communications providers would continue to be bound to adopt risk management practices. Other key players providing important inputs to economic and societal processes would not be required to do so.	0	High	3	Mandatory requirements for key pr sector players and pu administrations to analyse risks adopt adequate measures to face t risks would create a strong incentiv manage and dimension security effectively and in turn enh preparedness and timely response.

To ensure that NIS breaches with a significant impact are reported to the national competent authorities	Only electronic communications providers would continue to be bound to report NIS breaches. Other key players providing important inputs to economic and societal processes would not be required to do so.	0	High	3	Mandatory requirements for key pr sector players and pu administrations to report NIS incid with a significant impact w enhance transparency and enable ti and effective response. It would empower governments to con evidence-based policy making.
Total score Specific Objective 3		***0***			
Grand Total		***0***			

ANNEX 14: LIST OF ACRONYMS

BEREC Body of European Regulators for Electronic Communications

CCA Cross-sector Crisis Coordination arrangement

CERTs Computer Emergency Response Teams

CII Critical Information Infrastructures

CIO Chief Information Officer

CIIP Critical Information Infrastructure Protection

CIP Critical Infrastructure Protection

CISO Chief Information Security Officer

CNECT Communications Networks, Content and Technology Directorate General, (former Information Society and Media Directorate-General) of the European Commission

CSIRTs Computer Security Incident Response Teams

DG CONNECT Communications Networks, Content and Technology Directorate General, (former Information Society and Media Directorate-General) of the European Commission

DAE Digital Agenda Europe

DHS United States Department of Homeland Security

EC3 European Cybercrime Centre

ECIs European Critical Infrastructures

ECJ Court of Justice of the European Union

EFMS European Forum for Member States

EGC The European Government CERTs group

EISAS European Information Sharing and Alert System

ENISA European Network and Information Security Agency

EP3R European Public-Private Partnership for Resilience

EPCIP European Programme for Critical Infrastructure Protection

EU European Union

EU2020 Europe 2020 is the EU's growth strategy for 2020

EWRS Early warning and response system

FWD Framework Directive

FTE Full-time equivalent

GDP Gross Domestic Product

ICS Industrial Control System

ICT Information and Communications Technologies

ISACs Information Sharing and Analysis Centers

ISP Internet Service Provider

ISS EU Internal Security Strategy

IT Information Technology

MS Member States of the European Union

NACE Statistical Classification of Economic Activities in the European Community

NCI National critical infrastructure

NCP National Contingency Plan

NIS Network and Information Security

NRA National Regulatory Authority

PPPs Public-private partnerships

SME Small and Medium Enterprise

TFEU Treaty on the Functioning of the European Union