PSCE Response to the "IMPROVING NETWORK AND INFORMATION SECURITY (NIS) IN THE EU" Questionnaire

Many of the questions are related to concerns of individual enterprises, e.g., regarding the type of risk management approach they employ. Below are questions to which PSCE is able to provide an answer.

3.5. Do you consider that investing in a higher level of cyber security can be commercially valuable, e.g. because you can forestall reasonably foreseeable losses, or because you can make a good level of security a selling point (please explain)?

*PSCE considers that investment in cyber security can be of commercial benefit for organisations, both because it potentially mitigates losses caused by cyber-attacks **and** also because it has the potential to be used as a selling point. This is more so the case for organisations that operate in the critical infrastructure sector, such as electricity and gas provisioning. Furthermore, we argue that the processes followed by an organisation in order to ensure cyber security facilitate an organisation reflecting on the criticality and importance of its assets, for example, which supports business focus.*

3.7. Do you consider that governments in the EU should do more to ensure a higher level of cyber security?

- *Yes.*

3.8. If you have further comments or suggestions please write them in the box below.

There are a number of areas in which governments could take a more prominent role to ensure cyber security. For instance, a key factor in ensuring cyber security is education – governments could significantly help here by enhancing their education capability, both for public citizens and enterprises. Furthermore, on the matter of education, PSCE believe that cyber security should play a more prominent role in higher education programmes, for instance in computer science.

3.9. Information exchange between private companies and between the public and private sector on incidents, threats and risks is key to share best practices, build capabilities, develop trend analysis, manage risks effectively or reduce the impacts of incidents. What are the most effective ways to facilitate such exchanges at EU level (please explain)?

The ICT sector comprises informal networks which have proved very effective in information sharing, for example via CERTs. These existing initiatives could be improved, for example, through the development of tools for information sharing. Less developed on the other hand are information sharing capabilities between different sectors, e.g., between types of utility providers. Given the dependencies between these sectors, facilitating information sharing in this way, e.g., via cross-disciplinary training, tools etc, would be very useful. This is likely to become increasingly important due to future technologies, such as smart grids (and in the longer term smart cities of federated utilities).

3.10. What kind of incentives would be needed to make private companies and public administrations systematically report about cyber security incidents?

- *Notification and reports to the NIS*

3.13. In some instances, cyber incidents may result from criminal behaviour. Reporting cyber-crime is important to step up the fight against criminals operating on-line. How should this objective be achieved at EU level?

Although not in need of legal requirements to do so, everybody should be strongly encouraged to report incidents which appear to have criminal nature to law enforcement authorities.

3.14. If you chose the third option, please explain which incentives, other than regulatory ones, may be provided.

There are already incentives to report cyber-crime - for instance to maintain the trust of customers and the like. However, meaningful information that could be used by others, for example, to protect their systems is scarce. Arguably one of the reasons for this relates to the potential risks that are associated with information disclosure, which might render an organisation vulnerable. Insight into these risks and how they can be ameliorated should be investigated as a way of improving incentives to share information in this regard.

3.16. Everybody (business, consumers and governments) should ensure a minimum level of protection against cyber threats. Do you agree?

In part, yes. We agree that businesses and governments should ensure minimum levels of protection against cyber threats. Of course, consumers should be encouraged to do so too, but given the complexity of ICT systems, it is naïve to think one could ***effectively*** *legislate for this, among other issues.*

3.17. Which actions can be reasonably be expected to be taken respectively by business, consumers and governments to better protect themselves on-line?

For organisations such as businesses and governments, evidence of adopting an information security risk management approach should be given. Of course, this should not be a one-size-fits-all, e.g., an SME should not be expected to follow the same level of rigour as large utilities. Therefore, we encourage development of initiatives to address these various levels of risk management.

3.18. It is key to empower consumers and help them identify companies with good levels of cyber security protection. Which is the best way to achieve this objective?

- *Stimulate the development of industry-led standards at EU level*

- *Give guidance at EU level to enable consumers to differentiate good security products and services*

3.20. Raising awareness about cyber-security risks amongst business, consumers and governments and about the action that can be taken to better protect themselves is key to enhance security. Do you think that in the EU businesses and governments (through their employees) and consumers are sufficiently aware of the behaviour to be adopted to minimise the cyber-security risks that they face?

- *No*

3.21. If no, how can this objective be effectively achieved at EU level (e.g. a synchronised cyber security month in the Member States)?

A dedicated cyber security month in Member States could help to improve awareness of cyber-security risks. Another initiative could involve affordable access to basic cyber security training for employees – whether or not this should be enacted at an EU level is however unclear.

3.22. People driving a car are required to take security measures to protect themselves and others. Do you consider that people using the Internet should also be subject to security obligations? If yes, which ones?

No. PSCE believes it´s naïve to compare the complexity of maintaining the roadworthiness of cars to computing systems. The complexity of the problem is far greater considering the number of connected devices we each currently have and will have. Proving negligence in this respect would not be feasible.

3.23. It is important to ensure security throughout the supply chain. Which is the most effective way to encourage all actors in the value chain (e.g. product manufacturers, software developers and Internet companies) to invest in security solutions at an appropriate level?

Through the development of certification programmes that supply chain actors can look at in order to assess the degree of investment of an organisation in cyber security. In areas where there is limited competition, for example in the utilities domain, certification could be mandated.

4.1.6. For which sectors of activity would it in your opinion be important to adopt NIS requirements?

4.1.6.1. Banking and Finance - *Very important*
4.1.6.2. Energy - *Very important*
4.1.6.3. Transport (land, water, air) - *Very important*
4.1.6.4. Postal services - Important
4.1.6.5. Health (hospitals, medical/dental/nursing practices) - *Very important*
4.1.6.6. Water (supply, sewage, waste) - *Very important*
4.1.6.7. Manufacturing of ICT equipment - *Important*
4.1.6.8. Manufacturing of motor vehicles - *Very important*
4.1.6.9. Manufacturing of food, paper, chemicals, pharmaceuticals - *Very important*
4.1.6.10. Computer programming (software, data processing/hosting, web portals) - *Very important*
4.1.6.11. Internet services (e.g. commerce platforms, search engines, social networking, cloud computing) - *Very important*
4.1.6.12. Retailing - *Important*
4.1.6.13. Accommodation, food and supporting services (hotels, restaurants, travel agencies) - *Important*
4.1.6.14. Agriculture - *Very important*
4.1.6.15. Construction - *Important*
4.1.6.16. Professional & Scientific (accounting, engineering, R&D) - *Important*
4.1.6.17. Public administration (e.g. tax office, social security, land registry, education) - *Very important*
4.1.6.18. Culture & entertainment (libraries, museums, gambling, amusement parks) - *Important*

4.1.7. Would you in principle be favourable to the introduction of a regulatory requirement to manage NIS risks?

- *No*

4.1.8. If you have further comments or suggestions please write them in the box below

In general, PSCE is in favour of voluntary rather than mandatory regulatory introduction of measures, such as the management of NIS risks.

4.1.1.5. In your view, what proportion of incidents occurring in the EU is actually made known to the public or otherwise disclosed?

In our view, this can vary across the different sectors and is related to the scale of the incident in question. In general, we would suggest the number of incidents that are reported to the public is still relatively low.

4.1.1.6. Effective sharing of information on threats and incidents would be best achieved by:

- *stronger public-private cooperation mechanisms*

4.1.1.8. If a requirement to report NIS security breaches to the national competent authority were introduced, at what level should this requirement be set?

- *At national level to allow flexibility to the Member States*

4.1.1.9. If you have further comments or suggestions please write them in the box below

PSCE thinks the measures introduced by Article 13a, whereby actors must report incidents to their national authority first which are then summarised at a European level, is a good approach.

4.1.1.10. If a requirement were introduced at EU level, who in your opinion should be subject to it?

- *only business providing or using network and information systems underpinning services which are vital for the functioning of our society, such as transport, energy, finance, health, water and Internet services of general interest(e.g. e-commerce, search engines, social networking).*

4.1.1.11. If you have chosen the last option, do you consider that other limiting criteria for regulatory obligations are necessary (e.g. number of users, turnover, other)?

- *No, we think this should apply to businesses of all sizes in this sector due to their critical nature.*

4.1.1.13. If a requirement were introduced at EU level, should governmental bodies and public administrations (e.g. tax office, social security, land registry) be subject to it?

- *Yes*

4.1.1.17. If a reporting requirement were introduced, which incidents should be reported, i.e. how should the gravity of incidents be defined?

This very much depends on the sector the incident occurred in, for example, it may be important to report apparently relatively minor incidents in the critical infrastructure domain which could have significant societal impact. Another measure could relate to whether citizen's basic rights have been compromised in the incident, e.g.,, related to personal data.