NIS Platform

Minutes of the first Meeting of WG1 on Cybersecurity Risk Management

September 25, 2013; 10h00-17h00

European Commission

Brussels

1. Introduction

The Commission reminded the general objectives and the organisation of the NIS Platform and Working group 1. The NIS Platform is a key component of the European Strategy for Cybersecurity. It serves the 2 key priorities of increasing cyber resilience in the EU and developing industrial and technological resources for cybersecurity. The NIS Platform, and in particular WG1 and 2, will prepare the ground for the implementation of the proposed NIS Directive, which contains general obligations of risk management and incident notification for critical market operators and public administrations.

Guidance provided by WG1 and 2 should assist, for example, an Italian local electricity operator to appropriately manage the risks posed to the security of its network and information systems and to report the incidents which have a significant impact on the core services provided. A focus should be on SMEs and the sectors which are less advanced, to increase cyber security across the board.

The guidance provided by the Platform will feed into Commission recommendations on cybersecurity to be adopted in 2014. Such recommendations will establish a standard of diligence or duty of care which could, in the future, be taken into account when assessing the liability of an organisation following a cyber-incident.

The work of the Platform should draw from the working practices of the participants. It should follow a cross-sectoral approach and popose incentives for adoption.

The Commission explained that the objective of the first working group meeting is to establish the scope of work and the organisation of the group. The Commission does not chair the working groups, but entrusted members of the Platforms to steer the work of the groups. The Commission will make sure that the Platform works towards the general objectives it has set. It will further provide secretariat support to the chairs, with the help of ENISA.

The progress of each group will be discussed at the next plenary meeting of the NIS Platform, scheduled in December (date to be confirmed). WG1 and 2 guidance on risk management and information sharing is expected in spring 2014.

The working group chairs underlined the need to close gaps in terms of cybersecurity risk management. This requires reusing existing and known frameworks rather than reinventing the wheel. The chairs will focus on small organisations, while large organisations will also benefit from the work of the Platform. They intend to provide technology neutral conclusions. The work on incentives is important.

International companies like Iberdrola have experience in the US and will bring such experience in the discussion.

The chairs underlined the short timescale to issue the first output of the working group (6 working months).

2. Roundtable

A roundtable was organised during which each participant was asked to clarify his or her expectations and possible input to the work of the group.

Many participants explicitly welcomed the initiative and confirmed that they wanted to contribute to the work of the group by sharing their own experience. Several participants also explained that they wanted to build knowledge on risk management and learn from other sectors.

The participants underlined notably the following points:

- On risk management:
    - Several participants underlined the benefits of a risk-based approach; one participant welcomed the fact that the Platform followed a 'risk route' rather than a 'compliance route';
    - Several participants insisted on the importance of having a risk management framework that allows companies to cooperate;
    - One participant insisted that the risk acceptance factor of each organisation should be factored in;
    - One participant stated that security risk in software surpasses other risks; for this participant too much focus is currently put on network security, there is a need to take other risks into account;
    - One participant stressed that the assessment of risks is different from risk mitigation;
- On the organisations targeted:
    - Several participants welcomed the focus on SMEs; SMEs are part of the value chain, they need to be properly secured;
    - Participants notably underlined the need to raise awareness and promote risk management, in particular among SMEs; incentives are needed to promote the take-up of risk management; one participant mentioned the need to develop the cyber insurance market;
    - One participant noted that SMEs often outsource security;
    - Participants stressed the need to differentiate the risk management requirements of organisations by size / turnover;
- On the need to increase harmonisation (or interoperability):

- One participant stated that there is a need to build industry cross-sector knowledge as far as risk management is concerned;
- In particular some form or harmonisation, or interoperability, is needed to ensure security across complex supply chains; several participants stressed the need to secure the supply chain;
- One participant stated that risk management practices should be harmonised across the EU, but was concerned with sanction-based approaches;
- One participant mentioned the need to align the work of the Platform with similar initiatives at national level (e.g. ES); other participants added that consistency is needed across the EU and beyond;
- One participant claimed that an important aim is to achieve the single market; for that, standards should be promoted;

- On standards:
  - One participant warned that Europe should not build an island of standard, but aim for cooperative leadership in the field of standardisation, while another participant stated that the work of the group should be based on international standards;
  - One participant claimed that there are defects in the standardisation process, with too much bureaucracy involved; standardisation needs to meet business needs;
  - Several participants claimed that standards are not always easy to implement; assistance to implement them is welcome;
  - One participant stressed the need to take into account the NIST Framework (to be issued on 15 October);

- On the possible input to the group:
  - Several participants stressed the need to synchronise with other relevant initiatives, e.g. initiatives conducted in DG MOVE, HOME, or ENER; research results in particular should be shared; participants working on relevant research issues pledged to share the results of their work;
  - ENISA will provide input on risk management, currently available on the risk management portal;
  - One participant mentioned that best practices in counter-terrorism can be applied for civilian cyber-security; he mentioned that organised crime / cybercrime is a growing concern and should be taken into account;
  - One participant claimed that the development of cloud computing needs to be taken into account;

- On the output of the group:

- Several participants mentioned their opposition to the NIS Directive and to mandatory risk management obligations; they were concerned about the impact of the work of the Platform on the definition and the implementation of the NIS Directive; they see the NIS Platform as an important forum to develop voluntary rather than mandatory standards;

- Participants stated that the guidance provided by the group should be pragmatic, affordable and should permit innovation;

- One participant mentioned that instruments are needed to measure the adoption of risk management; other participants stressed that metrics should be promoted at EU level to obtain figures and statistics and to promote the adoption of cybersecurity.

The chairs thanked all participants for their input and recognised that there was a wealth of experience in the room. Key messages that had come out were that the resultant guidelines needed to cover:

- cross-border/cross sector and supply chain implications;
- all organisations, especially SMEs who have few resources or incentives to implement security requirements;
- a framework to address implementation, scalability and the means of measuring maturity against any standards used.

It was also clear that the working group should:

- not aim to "re-invent the wheel" but to build on previous work done;
- start by looking at existing guidelines and methods and identify potential gaps.

3. Discussion of the draft Rules of Procedures and Terms of Reference

Many of the points stated above were reiterated when discussing the objective, the scope of work and the output of the working group, in particular:

- The need to foster interoperability between risk management methodologies and practices; one participant claimed that the overall aim of the Platform should be to improve the interoperability of businesses in a safer way;
- The need to understand and factor in risk acceptance criteria;
- The need to make an inventory of existing studies, including ongoing ones, and the need to incorporate the work of ENISA on risk management;
- The opposition to linking the work of the NIS Platform to the NIS Directive, in particular:
    - Several participants claimed that the NIS Directive was not stable and therefore not a good basis for the work of the group; the Commission clarified that the reference should be the proposal of the Commission; the legislative process is dynamic, it is not possible to

take into account the different amendments proposed by the parties during the negotiation;

- Several participants claimed that the NIS Platform should work on developing voluntary standards and should be distinct from the implementation of the NIS Directive, which mandates risk management; if the group is tasked with defining mandatory measures, this could hinder participation; the Commission clarified that the output of the working group will be risk management guidance, which can be directly applied by stakeholders on a voluntary basis; it will be taken into account by the Commission to publish recommendations on cybersecurity best practices; the guidance from the NIS Platform and the Commission recommendations should help public and private organisations to comply with the general risk management obligation proposed under the NIS Directive; the NIS Platform is preparing the ground for the implementation of the NIS Directive;

Other general comments included:

- The need to develop standards that are re-usable and repeatable;
- Several participants claimed that harmonisation is politically loaded, they would prefer the term interoperability;
- The need to define more clearly what is risk, in particular the difference between external and internal risk, and what risk should be taken into account by the group;
- The need to take into account different types of risks, including enterprise and shared risks, and different types of threats;
- The need to define levels of assurance; the work of NATO in this area could be used;
- Several participants supported the idea of addressing maturity models;
- Some participants stressed that the work of the group cannot be technology-neutral, as many risk management processes are implemented through well-established technologies and this should be to be taken into account;
- One participant stressed that public sector purchases are a way to levy the risk appetite of the private sector;

The drafts proposed by the chairs were thoroughly discussed with the participants, who provided specific comments, including the following:

- The level of abstraction expected for the guidelines should be set in the objectives;
- A reference to the notion of proportionality as part of risk management should be added;
- The scope of work should be clearly linked to the objectives; the scope of work as described in the initial drafts is rather defining the output / the deliverables of the group; the development of risk metrics are an objective, not an element of scope;
- The organisations that are targeted should be mentioned;

- The role of the members of the group should be specified;
- The Information Assurance concept is no longer used; it is decided to replaced it by cyber security; references to NIS are also changed to cyber security;
- The drafts should identify the output of the group and the liaison to other WGs;

In terms of the organisation of work, the following points were discussed and / or clarified during the meeting:

- The work will take place on the basis of consensus;
- The meeting minutes and the deliverables will be approved by the chairs;
- The group will have to find ways to incorporate existing works, to avoid reinventing the wheel;
- Participants stressed the need to organise the work within smaller working groups;

The chair concluded the meeting, thanking the audience for their active participation and contribution. The chairs will incorporate the amendments discussed during the meeting to the Rules of Procedures and the Terms of Reference. The updated versions are considered to be signed off, following discussion in the first working group meeting. The exact working topics and the planning for delivery will be submitted to the group by the chairs.