NIS Platform

Minutes of the second plenary meeting of the Network and Information Security (NIS) Public-private Platform

December 11, 2013; 14h00-18h00

Brussels

1. Opening and Welcome

Gustav KALBE, Deputy Head of Unit of DG CONNECT Directorate H4, Trust and Security, opened the meeting and welcomed the participants.

Paul TIMMERS, Director of DG CONNECT Directorate H, Sustainable and Secure Society, thanked the participants for attending the 2nd NIS Platform plenary meeting. He welcomed the fact that such a wide audience is active and engaged in the process. He reminded the participants that the platform was launched six months ago and that 3 Working Groups (WGs) were subsequently created.

He explained that the three WGs address best practices in risk management for organisations - including Small and Medium Enterprises (SMEs); information sharing and incident notification approaches; research and innovation - including technologies and processes that are needed to address both mid- and long-term challenges in cyber security. He underlined that the scope of the work involved is huge and that the WGs should therefore set clear priorities. The proposed NIS Directive, which is currently being discussed by the Council and the Parliament, contains general obligations of risk management and incident notification. The NIS Platform will support the implementation of the Directive but also Horizon 2020 (H2020) and help increase their impact. Mr Timmers stressed that engagement and willingness from all participants is necessary to ensure pertinent input, based on their experience, current practices and knowledge.

He then explained that the three WG chairs would give an overview of the work carried out so far and the envisaged next steps. The aim of the plenary meeting is to assemble all the platform's participants to share the work and give further guidance to the WGs on the topics, priorities and possible areas of collaboration. He stressed that the coming weeks will be crucial, especially for WG1 and 2, seeing as they have to deliver their work by spring 2014. Given the strong audience and engagement, he was confident that timely delivery would be possible. He explained that the next plenary meeting is foreseen for April 2014.

Mr Kalbe presented the meeting agenda. In addition to the review of each WG's progress, two thematic presentations will be made, namely on ENISA's work on Article 13a of the Framework Directive and on cybersecurity related research objectives in H2020.

2. Report by ENISA on Art. 13a implementation work / guidelines

Marnix Dekker, from ENISA, provided background on major cybersecurity breaches and how they contributed to building the case for regulatory intervention in the field of Network and Information Security. He then gave an overview of Article 13a of the Framework Directive and ENISA's work to

support its implementation. The goal of Article 13a is to ensure security of electronic communication networks and services.

The Article 13a expert group is an informal and voluntary group of experts from national regulatory authorities meeting three times a year, chaired by ENISA and where the Commission is an observer. Among the topics discussed are the implementation of the Article, supervisory activities and the assessment of past incidents. Several tools have been developed, such as guidelines on incident reporting and minimum security measures and reporting tools, some of which were presented during the meeting. The aim is to provide Member States with guidance on appropriate security measures, commensurate to the risks, to strengthen collaboration between the parties involved and foster harmonisation in the Article's implementation across the EU.

Mr. Dekker underlined that security is a dynamic field, as technology and attackers' capabilities are rapidly changing. It is difficult to capture security in a static set of measures. The role of the regulators is to stimulate the adoption of cybersecurity best practices and to analyse incident reports and follow up.

3. Report on the progress of WG1 on risk management

Carl Colwill and Miguel Sánchez Fornié, WG 1 Chairs, took the floor to present the progress of WG1. Mr Colwill stressed the importance he places on receiving input from the plenary. He explained that although the WG had a slow start - it was difficult to get engagement and contribution - work was now progressing well. Highlights of the presentation include:

- Initial priorities: the aim is not to reinvent the wheel. There is a lot of experience and many best practices, so the idea is to identify the gaps, make pragmatic recommendations and develop incentives to get these best practices implemented. One of the challenges is to cover the work across organisations and across borders. Among the WG's priorities are risk management methodologies, risk metrics and their implementation (it has been identified as a possible issue for WG3), means of mapping cyber security risk management practices to the size and the particular risks faced by each organisation, and the use of capability maturity models.
- Progress: he presented the steps taken so far. The Terms of Reference (ToR) and Rules of Procedure have been issued; a huge amount of information has been shared on the ENISA portal – he stressed however that the most important part is not to upload documents, but to comment on them; the initial potential inputs to WG2 and WG3 have been discussed; gaps in membership have been identified – currently, participants mostly comes from large organisations in Western Europe, so further engagement from small businesses and Eastern countries is needed; three subgroups have been created – he thanked the leaders who have been very active. The issues dealt with in the subgroups are not separate per se, so close coordination between them is ensured.
- Next steps: It is important to issue recommendations that can and will be implemented. The ToR will be updated and reissued so as to define the remaining deliverables. The need to mobilise members to join and collaborate with the different subgroups was stressed. Finally, the WG will produce a detailed project and delivery plan to April 2014 and identify additional subgroups and subgroup owners.

Mr. Sánchez Fornié took the floor to underline that the WG must deliver operational guidance by April 2014: "there is such a degree of uncertainty in terms of cybersecurity that we need recommendations from experts quickly". He made a plea to the audience for more input.

Highlights from the following discussion include:

- The benefit of taking into account past cybersecurity incidents to identify risk management best practices;
- The need to build on ENISA's work and other relevant initiatives and ensure close coordination with other similar initiatives taking place simultaneously both outside Europe (e.g. NIST Framework) and at Member State or organisation level. Organisations which are taking part in several of these initiatives should propose ways to foster information exchange and coordination.
- The need to issue guidance on risk management swiftly. Even without considering forthcoming NIS regulation, organisations still need to prepare themselves to become more resilient. The worst case scenario of a cyber-incident affecting an unprepared organisation must be avoided.
- The Commission underlined that spring 2014 is not the ultimate deliverable. The guidance issued will focus on initial priorities set by the working group and will need to be developed further. It is essential to provide pragmatic recommendations.
- The Commission stressed that the operational guidance provided by the Platform would help the organisations concerned to comply with the obligations of risk management and incident notification contained in the proposed NIS Directive, once adopted and enacted into national law. The guidance should address only the implementation of the Directive's obligations and not the supervision of its application by national authorities.

4. Report on the progress of WG2 on information exchange and incident coordination

Mr Semple took the floor. Highlights of the presentation include:

- Structure and preparatory work: since the creation of the WG, WG2 Chairs have refined the ToR and agreed that the WG would look into guidance on best and good practices on information sharing and incident notification. They also agreed on the structure of the final output document. Meetings have taken place with private stakeholders and government representatives, as well as with industry bodies with legal or regulatory interest in cyber security and incident notification, in order to understand their experience.
- Direction statement: the WG will produce a paper on currently applied practices in information sharing and incident notification, at both the EU and international level. Based on this, WG2 will develop practical guidance.
- Next steps: the WG will now create subgroups on topics such as existing platforms, the practicalities of information sharing (privacy and trust are key issues), protocols and mechanisms for information sharing and services and incentives to promote adoption. Mr Semple stressed the importance of focusing on initiatives and developing services for SMEs and SMBs in particular. The WG will meet in January, review the content by the end of March, consolidate the draft by the end of April and have the final draft by the end of May.

Highlights from the following discussion include:

- The need to build on the experience of other sectors, especially on existing reporting schemes in the banking and airline sectors. Recommendations from the working group will seek to generalise principles that are common to current practices.
- The working group will seek to develop cross-country and cross-sector recommendations. For that the working group needs practical input from the different industry sectors. Several participants shared their experience of information sharing schemes at national or industry level in Europe (the CISP platform in the UK, the DENSEK project for a European energy ISAC, information sharing schemes between telcos and energy providers). The Commission invited participants to reach out to the working group and give their input.
- The question of liability linked to information sharing was raised. It will not be addressed by the working group in this initial stage. The working group should focus on providing operational guidance on information sharing and incident notification. The conversation should not move towards governance and regulatory processes. The Commission clarified that the issue of liability is not specifically addressed in the NIS Directive. It is up to the Member States to transpose the Directive and to address liability issues within their national rules.
- The focus of the working group is on information sharing and incident notification, not incident response coordination. Response coordination is rather an issue for the CERTs. Recommendations on standards and protocols will remain general and will not pick a winner.
- To get representation from SMEs, the Commission can assist the working groups to reach to European trade associations and invite them to the discussions. Another possible action is to ask the bigger organisations to get those SMEs which are part of their supply chains to participate. It was stressed that SMEs are the most exposed and vulnerable players, but they don't have the resources to look for and implement solutions. It is important to develop an approach commensurate to the size of the organisations. Giving incentives to SMEs may also help bring them in.

5. Presentation of the Work Programme 2014/2015

Mr Kalbe briefed the audience on the state-of-play regarding H2020 and the issues at stake in cyber security research and innovation. He reminded the participants that on 15 January, the Commission will organise an information day were the cybersecurity related research objectives in H2020 will be presented. He strongly encouraged participants to attend.

He stressed that under H2020 R&D is aimed at supporting policy. The cyber security policy is defined and implemented through the EU Cybersecurity strategy, which covers several areas: the international and defence aspects, cybercrime, resilience and technology and industry. The purpose is not doing research for its own purpose, but linking it with cybersecurity policy objectives. The idea is to help market operators develop technology, products and services that are necessary and more cost-effective. That's why the work of the platform is so valuable. There are legislative instruments to foster more resilience and security in Europe and this is complemented by a 'softer' industrial and technological approach.

Mr Kalbe underlined that cybersecurity research, development and innovation is not addressed in only one part of the work programme, but is actually a horizontal issue that can be found throughout various research objectives.

6. Report on the progress of WG3 on secure ICT research and innovation

Fabio Martinelli, WG 3 Chair, took the floor to present the progress of WG3. Highlights of the presentation include:

- Objective and scope: Mr Martinelli explained that the objective is to define and contribute to the coordination of European activities in secure ICT R&I. In this regard, the WG needs to identify key challenges and outcomes and foster a multidisciplinary and multi-stakeholder approach, in close coordination with WG 1 and WG 2.
- Composition: the group is composed of qualified experts willing to contribute. Initially, most of the participants were from industry, but the WG Chairs encouraged participation from academia, regulators, governments, etc.
- Working methods: the WG wants the work to be inclusive, value oriented, collaborative, coordinated, creative, transparent, neutral and simplifying things or problems. He explained that the main research topics for secure ICT should emerge from this WG. They divided the workload to improve efficiency. The WG meets regularly, usually through virtual meetings, with physical meetings for the main topics and adoption of milestones. It is a mix of bottom-up and top-down approaches.
- Main deliverables: the WG has identified three deliverables so far: "a snapshot of education and training", "business cases and innovation paths" and "the secure ICT research landscape in Europe". All this will feed into the strategic research agenda (SRA), which is the final outcome. The plan is to have the strategic research agenda by March 2015. There is one editorial team per deliverable and one more for the SRA.
- Steps achieved: One subgroup per deliverable was created and a first description of the SRA's Areas of Interest (AoIs) was done and is currently under revision. The WG has been using the ENISA platform to improve transparency and communication.
- Subgroups: the purpose and output of each of the subgroups were presented, as well as the draft tables of content for each deliverable. The WG also prepared a table of content for the SRA. It was stressed however that this is a living document, as it uses the other deliverables as inputs. There are overlaps between the subgroups, but they have been identified and will be addressed. The SRA will be drafted in three phases: parallel work on the AoIs in the subgroups; cross-analysis; final revision and polishing of the SRA. During the bottom-up approach, five main topics and hundreds of subtopics were identified. Now, in the top-down approach, they will define priorities.

Highlights from the following discussion include:

- The need to extract concrete R&D priorities after the exploratory phase is completed.
- The need to make sure that all organisations contribute to the work of the group. Contributions need to be concise and straightforward.

- The strategic research agenda prepared by the working group will seek input from all the groups working on R&D agendas in cybersecurity, including at national level. It will be the basis for the H2020 work plan. The document will outline the research priorities and their impact.

7. General comments and closing remarks

The WG chairs thanked the audience for their participation and feedback. They stressed the need for input from the participants, not only in terms of documentation, but above all regarding their views and experiences. They thanked the Commission and ENISA for their support.

Mr Kalbe concluded the meeting by thanking the audience for their participation and active contribution. He stressed that the process is quite challenging but worthwhile. He said that the meeting brought interesting feedback on priorities and questions raised. It is important to keep the momentum of this meeting. He welcomed that WG 1 and WG 2 focus on the implementation of workable solutions. It is important to do so before adopting legislation. He noted the importance of addressing the particular issue of SMEs, which are vulnerable but key players in the value chain, and the efforts made to include them. Harmonised practices will benefit cross-border organisations. He invited once again all platform members to contribute to WG3, even if they don't actively participate in it. He suggested that they all should list their three main real-life security concerns and send them to the WG. Finally, he stated that improving resilience is a valuable goal and a concern of everyone.