

## **NIS Platform**

### **Minutes of the third plenary meeting of the Network and Information Security (NIS) Public private Platform**

April 30, 2014; 10h00-16h30

#### **Brussels**

#### **1. Opening and welcome**

P. Timmers opened the meeting and expressed appreciation towards the work of the NIS Platform, in particular the efforts of Working Group Chairs and leaders of Sub-Groups in finalising the first set of guidance on good cybersecurity practices for risk management and information sharing/incident notification. Efforts should now go into starting to market the guidance, in particular towards SMEs, and use the feed-back for further improvement. The Commission is ready to issue public information, news items or blog posts to give visibility.

The guidance will also be an input into future Commission recommendations, that the Commission currently envisages issuing in early 2015. This is a bit later than originally foreseen in the Cybersecurity Strategy, which was to propose such recommendations in 2014. There are two reasons for this shift. Firstly, to cater for the need of the NIS Platform to further work on the guidance presented today. Secondly, to have a view on the final content of the NIS Directive and build positive synergy with its implementation.

It is important to keep eyes on the next deliverables of the Platform, on the research landscape and a strategic research agenda. In order to coincide with the ambitious timeline for WP 2016 preparations the more mature the strategic research agenda is by early autumn 2014 the better.

Regarding the future of the NIS Platform it will be important to identify the deliverables and plan the work for the coming six months accordingly and then match them with the necessary resources. Obvious topics would include a deepening of the guidance presented today. Regarding future ways of working of the Platform the idea of a Steering Group had been floated before the meeting but the intention is not to conclude the debate on this point during the meeting, rather to consider the discussion as a starting point. ENISA will step up efforts to support the Platform, through its expertise.

#### **2. Presentation of the guidance document of WG1 - risk management**

C. Colwill presented the guidance on risk management stressing that while it is a good starting point work still needs to be done for it to become mature. It may be necessary to start considering technology as well (so far aim has been to be technology-neutral).

Findings of WG1 include:

- Big gaps in effective frameworks and maturity models in risk management and their use. Very few standards existing on shared risk and dynamic risk. Hence standards, frameworks and maturity models need attention.
- The fundamental need to agree on the risk appetite and the link between risk appetite and tolerance levels. The risk appetite needs to be agreed within the frame of the NIS Directive.
- Controls should be driven by risk analysis, not by complying with a particular standard.
- Not easy to apply standards consistently across the supply chain.
- Remove barriers to uptake of best practices.
- Not to put too much emphasis on *predictive* risk management, it probably never will be.
- Best practices are not adopted, because they cost too much money.
- WG1 experience on process: Many organisations woke up only towards the end of the process, therefore all input from surveys has not been fully integrated into the current edition.

In the discussion members raised:

- The importance of linking any standardisation activities to work on international standards (e.g. US NIST is engaging with international standardisation organisations); the first meeting of the ETSI technical committee on cybersecurity at the end of May 2014 was mentioned as an opportunity to take this discussion forward.
- Why the economic reason (cost) for not adopting best practices was put as a question for future research. WG1 aware that incentives have been put in place.....but still not working additional research or research awareness factors to be applied.
- The difficulty of analyzing threats facing an organisation, because dependent on information that is secret or confidential.
- The mapping of standards against each other, building upon ENISA past work. The mapping of meta standards (c.f. US NIST Cybersecurity Framework) was mentioned as a helpful approach.
- That the use of standards should not raise new barriers. Some sectors outside the ICT domain (e.g. transport), and in particular SMEs, would face huge difficulties if compliance with standards were made mandatory (which is not the aim of the NIS Platform).

### **3. Presentation of the guidance document of WG2 – information sharing and incident notification**

W. Grudzien as Chair (the second Chair W. Semple, acted until March 2014), with A. Stockey and P. Curry of the sub-group leaders introduced the guidance of WG2, which for the moment has focussed

mostly on information sharing, with incident notification as a sub-set. Incident notification will be influenced by the outcome of the NIS Directive.

Findings of WG2 include:

- Guidance to SMEs will make sense only when regulatory requirements become clearer.
- Difference in industry and government preparedness, industries well ahead.
- Difficulty to assess the number of existing information sharing schemes. WG2 Survey did not give comprehensive overview. Based on the limited responses received the tendency of schemes is towards national, voluntary schemes with less than 20 participants. **Need to establish catalogue of information sharing schemes, together with ENISA. This could be further developed into a catalogue of collaborative requirements.**
- Having standardised data models would facilitate the scaling of information sharing schemes. To be noted that there are already more users of international standards in Asia than Europe and US combined.
- To compare with existing maturity models for schemes (e.g. US DHS).
- Recent incidents (e.g. Target) has shown need to establish new schemes in sectors such as retail that are not traditional critical infrastructure.
- A barrier to information sharing is the need to guarantee the protection of personal data. NIS Directive and proposed Data protection regulation recognise it to some extent, but important to get it reflected at MS level. **Need for guidance on how data protection rules should be applied in situations of information sharing.**
- The current tendency towards increased transparency and control through regulation diminishes the incentive of industry to establish trust and take responsibility through information sharing in communities. Need to find a way to align public policy and business interest.
- Recommendations for operation of information sharing schemes could address the operation of voluntary public-private information sharing schemes, conditions for access, how schemes operate (e-mail, phone conversations).

#### **4. Report on progress of WG3 – Secure ICT research and innovation**

R. Riesco Granadino provided an update of WG3 work towards their different deliverables in 2014: the research landscape (available for comments at ENISA platform), business cases & innovation paths (on-going), the education & training snapshot for workforce development (on-going) and a strategic research agenda (SRA) which is structured in 3 different Areas of Interests (AoI) which are on-going as planned. He also commented that valuable research needs have been received by WG1. He confirmed that the WG3 is on time to deliver a first consolidated version of the AoIs of the SRA in the Autumn, in time for H2020 future WP discussions, as outlined by P. Timmers.

## 5. Discussion on future topics and working methods of the NIS Platform

J. Boratynski introduced the discussion by referring to the set of questions that were circulated before the meeting (in attachment) and were intended to guide the discussion.

He also reminded that the intention was not to conclude on this discussion during the meeting, but that it would feed into the reflection.

Issues and suggestions raised:

- Recognise that the first delivery of WG1 and WG2 guidance is already a big step forward.
- Questions were asked on the status of the NIS Platform guidance document. J. Boratynski reiterated the message of P. Timmers that the Commission would give visibility to the NIS Platform guidance and that the question of how to use it is part of the discussion, bottom-up driven process. From the WG presentations there is a feeling that there is further work to be done within WG1, that WG2 is in the process of reflection and that WG3 is progressing towards delivery within the timelines.
- Questions were asked on the form that future Commission recommendations would take. J. Boratynski clarified that NIS Platform guidance are key inputs to the recommendations to the extent that those involved in the deliverables recognize them and feel ownership. But formally the Commission recommendations are separate from the NIS Platform output.
- The lack of consensus for the NIS Platform guidance. One participant stated that comments had not been taken into account. There is a need to have more meetings/workshops in person, more time in drafting documents.
- The need to have enough resources devoted to the work, human resources, meeting occasions and funding of travel in particular for SMEs.
- SME's difficulty in applying standards, which is a model that works for big companies, but not for smaller ones. The only incentives that truly work for SMEs are money, tax benefits, vouchers.
- WG1 idea to launch a pilot group of SMEs trying out ideas.
- Pick topics where public and private share goals.
- Call for governance model and appropriate funding. Clarify where NISP input is sought for the Directive. More need for technical authors than reviewers, which has been the case so far. The importance of regular outputs (e.g. every 3 months) to keep momentum was also mentioned.
- Call for visibility for presented documents, even if does not reflect consensus. Call for delivery plan for next steps and deliverables.

- No mechanism for consensus building. Use ENISA experience in running stakeholder network. ENISA governance model in EP3R included a steering committee and funding, clear framework and focus that can be measured.
- Link with Art 13 Telecom framework directive.
- Clarity on how input will be used, whether it is at the level of strategy, regulatory, technological foundations, this will steer the nature of input. Chain of event to achieve impact – deliverable – dependencies – follow up.
- Not to duplicate what other groups are doing (e.g. standardisation, ETSI).
- Importance of cyber assurance, that systems are secure, software analysis.

J. Boratynski resumed by restating that Commission cannot take ownership for output of NIS Platform directly. Document will be published by ENISA on the NIS Platform space, Commission will refer to it to give visibility. Further work will be needed to make them more mature and more endorsed, as guidance and input to Commission recommendations.

#### **6. External presentation by FERMA (Federation of European Risk Management Associations) on the potential use of NIS Platform guidance, e.g. for cyber-insurance purposes**

J. Bedhouche introduced by outlining that cybersecurity, from a risk managers' point of view, is still an emerging risk. At the outset it is regarded as purely an IT risk, but now recognised as enterprise risk, within the scope of risk managers. Important to establish link between operational IT department and company board. NIS Platform guidance is very useful to 'talk the same language' but FERMA would be cautious about kite marks in a dynamic area like cybersecurity. Barrier to standards is the sharing of IPR, while we are at the stage of sharing best knowledge. Standards produced are typically disappointing. Government-backed standards are too simple. Not fit for SMEs. Guidance documents are quickly getting old.

Some recommendations from risk managers' point of view would include:

- Redefine communication and reporting line, between IT and Board.
- Cyber is not a traditional risk, with actuarial data, still complex to define and price. But offering is expanding rapidly. Shortcoming that bodily injury and property damages are currently excluded from coverage.
- Determinant for insurance is risk exposure, that role cannot be taken over by certified schemes or labelled. Same scheme or metrics will not suit companies with very different risk exposures, from consumers' financial data to design-led businesses.
- Shortcoming for critical national infrastructures, which are not covered, take inspiration from terrorist risk insurance acts (US), or ones governing natural disasters (FR).

- Independent risk assessment is becoming requirement for underwriting and a condition for 3<sup>rd</sup> party suppliers.
- Cyber insurance is an umbrella insurance. A gap analysis against existing insurance policies is needed for each organisation to understand what coverage is needed. May be suitable for the residual risks. Completing a cyber insurance form is a worthwhile exercise, even if it is not taken in the end.
- Cyber insurance is not a substitute for effective and efficient risk management.

## 7. General comments and closing remarks

J. Boratynski concluded that WG documents will be published with appropriate caveats. If members feel there are important issues to be raised they should be raised within the timeline that Commission will set. Questions on deliverables, resources, governance have been raised. Regarding the purpose of NIS Platform work the initial line remains, that it should help in implementing the NIS Directive. Commission will hold conference call with ENISA and Chairs to reflect on the way forward. **The intention is to come back to the NIS Platform membership before the Summer with a proposal for way forward.** Next plenary possibly in Rome late October 27-30.10, joint event with IT Presidency, but to be confirmed. ENISA will be more involved in the process in the future.

## **Attachment, e-mail circulated before the meeting on the future of the NIS Platform**

The NIS Platform Plenary meeting 30.4 will mark an important first milestone for the Platform, with the presentation on WG1 and WG2 guidance. It is therefore opportune to take the opportunity of the Plenary meeting to discuss future topics and working methods for the Platform.

- **What work needs to be undertaken in order to further mature the WG1 and WG2 guidance presented on 30.4?**

Sector-specific considerations, uptake with SMEs etc.

- **Should the Platform undertake new areas of work?**

Incentives such as labels, public procurement, cyber-insurance and other topics mentioned in the Cybersecurity Strategy and so far put aside, due to time and resource constraints

- **Should the Platform broaden its focus ?**

The EU Cybersecurity Strategy also tasked the NIS Platform to identify factors that could contribute to the adoption of security standards and solutions, to apply them to ICT products used in Europe as well as to possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. This strand might necessitate changing the focus of the NIS Platform from dealing with *existing* standards to examining the need for *new* standards for secure products and services and the certification against such standardised requirements. ENISA is ready to introduce this topic to the NIS Platform at a future meeting.

- **Comparing approaches internationally?**

Other regions of the world are also putting in place regulatory and voluntary approaches to deal with cybersecurity risks. Should the NIS Platform engage in work to compare approaches of other countries such as the US and possibly others, based on the NIS Platform guidance?

- **Awareness raising**

The European Cybersecurity Month will take place in October 2014, with a kick-off event in Brussels on 1.10.2014. NIS Platform Members should take this opportunity to liaise with ENISA and their national coordinators in order to maximise messaging opportunities during the month.

- **Should the working methods of the NIS Platform be adapted, in what way?**

E.g. by establishing a Steering Group (Commission, ENISA, industry, governments, academia), which engages with the wider community in the different WGs as appropriate