NIS Platform

Minutes of the first Meeting of WG2 on Information Sharing and Incident Coordination

September 26, 2013; 10h00-17h00

European Commission

Brussels

1. Introduction

The Commission reminded the general objectives and the organisation of the NIS Platform and Working group 2. The NIS Platform is a key component of the European Strategy for Cybersecurity. It serves the two 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 WG2, 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. In this regard, the priority of WG2 should be to help public and private organisations to report cybersecurity incidents to public authorities. 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.

The work of the Platform should draw from the working practices of the participants. It should follow a cross-sectoral approach and propose 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 WG2 guidance on risk management and information sharing is expected in spring 2014.

The Chairs welcomed the participants and stated that their aim was to have an open discussion, with a view to gather ideas from the audience on the relevant areas of work, to complete the draft Terms of Reference and focus the scope of WG2.

There were questions from the audience on the link between the NIS Platform and the NIS Directive, on the expected outcome and impact of the NIS Platform and on the focus on SMEs vs. critical infrastructures. One participant mentioned that mandatory incident notification had been criticised by a recent study commissioned by the European Parliament.

The Commission reiterated that the NIS Platform should assist and prepare the ground for the implementation of the NIS Directive, by identifying best practices that can be adopted by the companies which will be subject to the obligations of risk management and incident notification set out in the Directive. WG2 should provide practical guidance on how to share incident information with public authorities. The focus on SMEs stems from the fact that SMEs are often less advanced and need guidance to increase their level of cybersecurity. Many SMEs manage critical infrastructures and will be concerned by the obligation to notify cyber security incidents. Finally, the Commission noted that there are studies which support mandatory incident notification. Moreover, the need for mandatory incident notification does not seem to be contested in the current debate at the European Parliament. The work of the group is to identify best practices to notify incidents, which would still be useful in case of voluntary reporting.

One participant asked whether cybercriminal threats would also be taken into account in the work of the group. The Commission confirmed that the objective was to increase cyber resilience and therefore all types of threats and incidents, be it intentional or non-intentional, should be taken into account.

2. General comments

The Chairs opened the floor for general comments on the central theme and the scope of work of WG2. One of the Chairs mentioned that, in his experience, information sharing had allowed his company to become more proactive. The issue is the risk of leakage.

The participants made the following comments:

- UK telcos share information on cybersecurity; there is a need to share information on personnel issues as well, which requires trust; sharing information with competitors involved is a major challenge;
- A key question is when to share data; the Chair mentioned that there are different thresholds, which are difficult to align;
- The importance of sharing during incidents was underlined;
- Sharing information on threats is seen as the most difficult part of information sharing;
- Anonymous sharing is also an option, e.g. supported by traffic light protocol; but relevant information can be lost when sharing anonymously;
- Ad-hoc sharing based on person-to-person communication (e.g. emails) is also useful; in the future bulk information will be shared;
- Some participants claimed that cross-sector sharing is very important, while others do not see the benefit of it;

- There was a suggestion to test information sharing as part of WG2; operational / concrete work could be useful; the Commission clarified that the focus should be on identifying best practices;
- There was a call to define a taxonomy, a common language for information sharing;
- Possible maturity models should be suggested by the group;
- The group should discuss barriers to information sharing beyond privacy and trust;
- There is a need to foster re-use in case of reporting to different public authorities;
- WG members present across the Atlantic will provide feedback on information sharing in the US.

3. Privacy and trust and barriers to adoption

The Chairs asked about the behavioural barriers to information sharing, including the barriers to trust and the solutions to overcome them. The participants discussed the following barriers:

- The difficulty to share information with unknown parties and the need to ensure the confidentiality of the information; one participant mentioned that trust might also be an issue within an organisation;
- The lack of security policy in certain organisations;
- The difficulty to share with certain industry sectors (e.g. media) and the importance of non-disclosure agreements;
- The difficulty to share with competitors;
- The fact that information sharing (e.g. with suppliers or customers) can have a negative commercial impact;
- The fact that all countries are not equally trustworthy;
- The possible asymmetry in the benefits of information sharing;
- The fact that national privacy laws sometimes prevent sharing, due to potential high fines in case of unlawful transmission of personal data;
- One participant mentioned that the basis for sharing information is not trust but a cost/benefit analysis; mandatory information sharing has a cost;
- The possible sanctions (in the form of fines or new regulation) following from sharing with government can be an impediment; government's transparency may also hinder reporting;
- One participant mentioned that telcos are under the obligation to report incidents under Art. 13a FD; the information is used by ENISA to produce an annual incident report; he asked whether the plans of the Commission under the proposed NIS Directive were to extend this mechanism or to

have a reporting centre at European level with operational capabilities; the Commission replied that the objective of the NIS Directive was to extend the obligations which apply currently only to telcos to other critical market operators and public administrations; the NIS Directive further proposes to implement EU-level cooperation between the NIS competent authorities, including exchange of information and coordinated response.

On the solutions to build trust and foster information sharing, the participants made the following suggestions:

- On building trust:
    - Trust relationship between companies is often in fact trust between individuals: when one leaves, the 'trust bond' is gone; company agreements are a proper answer to this, there is a need of binding agreements, including non-disclosure agreements;
    - It is important to make sure that the information does not go to the wrong person inside an organisation; how information is disclosed or discoverable is a crucial point to establish trust;
    - It should be possible to assess the capability of other organisations to protect information;
    - It is important to decide who joins / who does not join an information sharing platform;
    - One participant suggested to build communities where there is trust, like between nations; practices to establish trust between nations can be re-used; need to govern the attributes of trust, the assurance of trust and awareness;
    - Fidelity of information, and its completeness can build up trust, or hinder it; chains of trust and fidelity of information are essential;
- On fostering information sharing:
    - There is a positive externality in information sharing: the more people share, the better; in this regard, several participants underlined the importance of two-way sharing; reciprocity of sharing is an incentive to share;
    - One participant mentioned the need to leverage on embarrassment ("I had an incident") to foster reciprocity of sharing;
    - Certain participants insisted on the need for accountability and even sanctions as part of information sharing mechanisms;
    - Several participants claimed that they preferred voluntary sharing; defining the parameters of mandatory sharing (e.g. thresholds for incident notification) is difficult; one participant claimed that information should be shared on vulnerabilities rather than on incidents;
    - One participant referred to the specific problems the shipping industry encounters with cybercrime; it is essential to discover and share the methods of the enemies;

- Participants stressed the need to raise awareness on the benefits of information sharing; to develop a taxonomy of information sharing; to develop a model for trusted information sharing;
- On SMEs, there was consensus on the fact that SMEs do not share or under-report; it is challenging to share between large groups of SMEs; anonymous sharing could be a solution; one participant stated that if the objective is to increase the overall level of security, the fact that SMEs only consume information should not be an issue.

3. Frameworks and Protocols

The Chairs opened a discussion on the frameworks and the technical protocols that facilitate the mechanism of sharing, asking for feedback and recommendations on existing and used frameworks.

Different frameworks and protocols were discussed, including the Common Vulnerability Report Framework (CVRF). Participants underlined:

- The need to create a taxonomy to standardise threat categories; the Chair mentioned that WG3 could help in this regard;
- The importance of use cases;
- The need to take into account the specificities of sectors;
- One participant mentioned the EU-funded ACDC project, which will provide a framework for coordination and cooperation between EU Member States, private sector organisations and international partners;
- ENISA mentioned its centre of trust for Art. 13a FD.

4. Approaches to adoption of information sharing

The Chairs underlined that security being a non-competitive factor, incentives are needed to foster information sharing and improve the overall level of cyber-security. Participants made the following suggestions:

- Make incident reporting easy, e.g. use similar templates to report to different authorities;
- One participant stressed the need to have no penalties, no consequences from incident reporting;
- Encourage sharing, e.g. 'October share' during the cybersecurity month; organise exercises so that stakeholders know what to do with the information shared;
- Encourage cyber-insurance and risk distribution; this is currently still embryonic;

- Adapt the information sharing business cases, e.g. to address the needs and challenges of SMEs;
- Increase awareness and education;
- Use information sharing platforms in exercise.

One representative from the postal sector mentioned that the postal sector expresses now greater interest in cyber security and risk management. The postal sector is turning its attention to online risks in addition to sector-specific and physical risks (e.g. secrecy of correspondence, terrorism, fire).

5. Conclusion and next steps

The Chairs thanked the participants for their active contribution during the day. They mentioned that they would re-draft the Terms of Reference to incorporate the comments of the participants.

The Chairs insisted that given the short delay to prepare the group's first output, maximum re-use of existing material will be needed. In a first phase, the working group will focus on collecting information. Several participants volunteered to provide input on existing information sharing platforms and protocols. ENISA pledged to provide links to relevant studies and information on the platforms under its responsibility.

Future work will be shared between sub-groups. Conference calls will happen on a sub-group basis.

The Commission thanked the participants for having shared insights about working practices and real-life barriers to information sharing, including lack of trust, and to have kept the focus on SMEs and stakeholders which are less advanced or less aware of cyber risks. Several participants stressed the benefits of sharing across sectors, which validates the horizontal approach of the group. Sector-specific guidance could be considered at a later stage. The Commission took note of the importance of facilitating reporting to different authorities, an issue which the group could help resolve, and of the importance of two-way sharing.

The Commission thanked participants for their active contribution, stressed that real work is starting now and asked participants to share input as agreed. The chairs will decide on the precise organisation of work and the next steps and will share their proposals with the group.