WG2 - Recommendations and Guidance for Information Sharing

Waldemar Grudzien
William Semple

4 December 2013

1 Introduction

1.1 Overview

The creation and establishment of a Network and Information Security public-private Platform to identify good cybersecurity practices was announced as part of the Cyber Security Strategy of the EU.

The NIS Platform will help European stakeholders to carry out appropriate risk management, establish good cyber security polices and processes and further adopt standards and solutions that will improve the ability to create safer market conditions for the EU.

Working Group 2 (WG2) has been established to promote the sharing of cyber threat information and incident coordination in both the public and private segments of the EU. It will identify requirements and issue recommendations on sharing cyber threat information as well as appropriate incident management processes in order to better prevent and best respond to cyber incidents.

1.2 Scope

WG2 will assist and provide the groundwork for the implementation of the information sharing and incident response measures set out in the proposed NIS Directive.

WG2 will investigate the feasibility and needs to address the ability for an organisation to share cyber threat information and to utilise a standard incident management process.

This will cover both public and private organisations, and all industry verticals within the private sector.

The primary focus will be with CNI (Critical National Infrastructure) organisations in the Private sector and Public sector organisations with mature and established threat and incident management processes. This will allow WG2 to gather existing working practices that have been used at an operational level with an intention to consolidate themes, common practices and successful information sharing practices.

It will also allow WG2 to establish some of the concerns associated with information sharing and how they were overcome. An example of this is in the Financial Services sector where the sharing of cyber threat information is an established practice.

Included in the scope is the possibility of developing the SME and SMB capability in cyber security and how these sectors can benefit from the recommendations and guidance for Information Sharing developed by NIS platform WG2 (see Section 6) without being overly burdened by mandatory requirements.
One aim of the EU Strategy on Cyber Security is help develop safer market conditions in the EU and create a supply chain that has capability to withstand cyber threats. To do this we must consider the SME and SMB sectors.

The sharing of cyber threat information for a SME or SMB organisation can seem like a daunting prospect. Included in the scope of WG2 is the concept of early adopters and mentor status. This is where we would consider the approach of more mature and experienced public and private organisations becoming early adopters of the recommendations of NIS Platform WG2 and working within their supply chain, industry vertical or geography to identify SME or SMB organisations that they can assist and mentor in the development and adoption of Cyber Security good practices.

The technical elements of the scope of WG2 will look at the standards, protocols and processes available and in use by public and private sector organisations. It will also look at any similar national level initiatives that are being considered in other regions such as North America, APAC or Africa.

Finally WG2 recognises that privacy and trust are major considerations for any information sharing platform. WG2 will look to capture issues, concerns and possible working models that address privacy and trust in the sharing for cyber threat information.

1.3 Objectives

The following will be listed as objectives for Working Group 2:

1. Understand implications of EU Cyber Security Strategy on WG2
2. Correlate Information sharing practices used by public and private sector organisations
3. Provide guidance and recommendation on Privacy and Trust
4. Proposed Frameworks and Standards to be used for Information Sharing and incident coordination
5. Approach to Adoption of Information Sharing
6. Gather information on similar initiatives in other regions for considerations on interoperability

1.4 Deliverables

WG2 will deliver an outcome document which covers the following topics:

1. Analysis of Information Sharing practices in use in the public and private sectors currently
2. Guidance on Privacy and Trust with Information Sharing
3. Proposed Framework and Standards to be used for Information Sharing and Incident Coordination and approaches to adoption
4. Report on similar Information Sharing initiatives in other regions

2 Existing Sharing Platforms

2.1 Analysis of Information Sharing practices

To do: Please describe "your" country with the characteristics
This chapter contains an analysis of Information Sharing practices in use in the public and private sectors currently. Examples for cooperative models for effective Public Private Partnerships are taken from [ENISA 2011-2], Chapter C.4.

To do: Each country mentioned in [ENISA 2011-2] Chapter C.4, with the characteristics:
- Which communication means are used before/in incident/crisis?
- Membership/Notification/Anything else mandatory?
- Group of participants, amount of participants? All sectors? CI-sectors only? Single sectors?
- One group (plenary), one group with subgroups?
- One SPOC for all?, many SPOCs? Direct communication (member to national body)?
- Who is the spider in the net?
- Means for trust and data privacy for information sharing?
- Seniority of members?
- Governance available?
- Criteria for Severity and Reporting
- Further topics

2.2 National Platforms

2.2.1 Austria

CERT-AT. In the case of significant online attacks against Austrian infrastructure, CERT-AT will coordinate the response by the targeted operators and local security teams. CERT- AT is the primary contact point for IT-security for Austria at the national level.
http://www.first.org/members/teams/cert_at/
Recall Austrian member/s of WG2

A-SIT The Secure Technology Information Centre. Its mission is to provide concentrated support of IT security issues for public institutions and the economy.
http://www.a-sit.at

Recall Austrian member/s of WG2

2.2.2 Belgium

BENIS* The Belgian Network of Information Security. This platform brings together the federal institutions involved in making policy on the security of information. It also supervises three working groups: "Classification of Information", "Critical Information Infrastructures" and "Harmonisation of the Functions Linked to the Security of Information".
(Web page not located)
Recall Belgian member/s of WG2

2.2.3 Estonia

Computer Protection 2009 is a joint project of the Look@World Foundation and the Ministry of Economics and Communications. The Look@World Foundation was established in 2001 by ten leading companies in Estonia with the goal of fostering the development of the IT society in Estonia. The Computer Protection 2009 project (also called Look@World 2) aims to foster the security of the Estonian information society.
http://www.riso.ee/en/node/80

Cooperative Cyber Defence Centre of Excellence (CCD COE)
Located in Tallinn, Estonia, the Centre is an international organisation that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, the Slovak Republic, and Spain as Sponsoring Nations. It is open to all NATO nations. Its mission is to enhance the capability, cooperation and information sharing among NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.
http://www.ccdcoe.org/37.html.
…

2.2.4 Finland

NESO* The National Emergency Supply Organisation includes a planning committee network of clusters and pools that are Public Private Partnerships. The clusters, which focus on priority areas for Finland's security of supply, are broad-based, sector-specific collaborating organisations consisting of experts representing the authorities, relevant bodies and the main parties involved.
http://www.nesa.fi/security-of-supply/public-private-partnership/

Ubiquitous Information Society Advisory Board
The Ubiquitous Information Society Advisory Board is a body with members from ministries, public administration, NGOs, and business life. Its task is to ensure that the National Information Society Strategy will be put into practice.
http://www.arjentietoyhteiskunta.fi/inenglish
…

2.2.5 France

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) created in 2009. The agency will operate a centralised capability to detect and defend against cyber-attacks. It will have the resources to sponsor the development of, and acquire, the security products essential to protect the Government's most sensitive networks.
The agency will also take on an advisory role to the private sector, particularly in areas of critical strategic importance, and will participate actively in the development of security for the information society.
http://www.ssi.gouv.fr
…

2.2.6 Germany

Both private and public worked together to develop the CIP Implementation Plan - Umsetzungsplan KRITIS (UP KRITIS) that was adopted in 2007. It is the foundation for a long-term partnership between the public and private sectors. Its three strategic objectives are "Prevention, Preparedness, Sustainability".
http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/cip_stategy.pdf?__blob=publicationFile
Mr Jendricke/Grudzien

2.2.7 Italy

Italy has a working group on critical information infrastructure protection, established in 2003 as part of the Prime Minister's Office that composed of representatives from Government departments and agencies, and private sector operators.
http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&Itemid=99
…

2.2.8 Netherlands

ECP-EPN, the Electronic Commerce Platform and the Platform for e-Netherlands, is a non-profit platform, working with member organisations from government, industry and science on all aspects of e-Netherlands.
www.ecp.nl

The NICC, (National Infrastructure against Cybercrime), is an organisation at the heart of the Dutch National Infrastructure, which brings together a select group of government services and representatives of critical industry sectors to collaborate in the fight against cybercrime. The model comprises various consultation groups in which representatives of companies exchange confidential information with each other on a per-sector basis.
www.samentegencybercrime.nl

NCO-T* The National Continuity Forum Telecommunications (NCO-T) has the objective to develop a way to implement the obligations put down on telecom operators in the Netherlands. It addresses the preparations to be made by an operator to be able to operate critical telecommunications services during a situation of Exceptional Circumstances.
www.nis-summer-school.eu/nis09/presentations/11a-Merkom.pdf

…

2.2.9 Norway

NorCERT (Norwegian Computer Emergency Response Team) coordinates preventative work and responses against IT security breaches aimed at vital infrastructure in Norway. They alert of serious attacks, threats and other vulnerabilities related to serious IT security.
https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT/English/
…

2.2.10 Poland

ARAKIS-GOV is an early warning system reporting threats arising on the Internet. The system has been developed by the IT Security Department of the Polish Internal Security Agency in cooperation with the CERT Polska team operating within the NASK organization.
http://www.cert.gov.pl/portal/cee/39/78/ARAKISGOV_system.html
…

2.2.11 Spain

The National Centre for the Protection of Critical Infrastructure (CNPIC) is the leading and coordinating office for every activity related to the protection of critical infrastructure.
CNPIC has aimed its efforts clearly towards critical infrastructure protection from a holistic point of view, by
integration of physical and cyber security in a single scope.
http://www.cnpic-es.es/
…

2.2.12 Sweden

PTS is the Swedish Post and Telecom Agency, which monitors the electronic communications and postal sectors in Sweden. The Agency works with consumer and competition issues, efficient utilisation of resources and secure communications. One PPP within the PTS is the National Crisis Management Co-ordination group (NTGC) that has been trained to be able to function in a national emergency, to test and develop the forum, to update documentation, to develop contacts and to coordinate exercises.
http://www.pts.se/en-gb
http://www.pts.se/en-gb/About-PTS/Information-materials/
…

2.2.13 Switzerland

Within MELANI, the Reporting and Analysis Centre for Information Assurance, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures.

It plays a role in all four pillars of the Swiss information assurance policy (prevention, early warning, crisis management, and technical problem solution) and is the central office for CIIP in Switzerland.

The "closed constituency" of MELANI can be described as a dedicated Public private partnership for CIIP.
http://www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=en
…

2.2.14UK

CPNI Centre for the Protection of National Infrastructure. Government authority that provides protective security advice to businesses and organisations across the national infrastructure.
http://www.cpni.gov.uk/

The UK Network Security Information Exchange (UK-NSIE) formed in April 2003 to share sensitive information in the information and communications technologies sector. It currently includes IP providers, core mobile operators, and traditional telecommunications providers, as well as CPNI. Participating companies now cover over 80% of the telecommunications market in the UK. It is linked to NSIE in USA, of which BT is a member. BT acts as the channel for information between the two Exchanges. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include a guide to the procurement of resilient telecoms and best practice guidance on the secure implementation of BGP.
nsie@cpni.gsi.gov.uk

EC-RRG Electronic communications resilience and response group aims to ensure the availability of Electronic
Communications infrastructure for the UK and provide an industry emergency response capability through the ownership and maintenance of the National Emergency Plan for Telecoms. They take the lead in developing and maintaining cooperation between the telecommunication industry and govt. organisations.
http://umbr4.cabinetoffice.gov.uk/media/200048/ec-rrg_tor.pdf

WARPS, Warning, Advice and Reporting Point
A WARP is a cost-effective, community-based service where members can receive and share up-to-date advice on security threats, incidents and solutions. This community is supported by a WARP operator. A WARP provides a trusted reporting point mechanism for sharing security incidents and other sensitive information without fear that the information will be used against them. Pooling and sharing this information with other members of the WARP, and possibly other WARPs as well, leads to more robust and secure systems.
www.warp.gov.uk.
…

Cyber-security Information Sharing Partnership

UK approach to sharing Cyber Security risks and incidents
Ashley Jelleyman, B.T.

2.3 International Information Sharing initiatives in other regions

2.3.1 US

To do GE/Verizon ?

2.3.2 ARECI workgroups

The Study on Availability and Robustness of Electronic Communications Infrastructures (ARECI) was conducted for the European Commission. The Final Report of the ARECI Study presented ten Recommendations to European Institutions, Member States and Private Sector stakeholders. In order to carry out some of the recommendations, workgroups were set up combining public and private stakeholders, who worked together to enhance the availability and robustness of Europe's communications networks.
http://www.epractice.eu/en/library/281377
to do by whom?

2.3.3 ETSI

is recognised as an official European Standards Organisation by the European Union, enabling valuable access to European markets. They produce globally applicable standards for Information & Communications Technologies including fixed, mobile, radio, broadcast, internet, aeronautical and other areas.
http://www.etsi.org/WebSite/homepage.aspx
to do by whom?

2.3.4 FS-ISAC

Mr Stockey ?

2.4 Industry Verticals

2.4.1 Sharing of Information within the Mobile Telecommunications Industry

Martin Peylo, Nokia Solutions and Networks

3 Information Sharing

We need to identify a Sub Group for Section 3.
Researching and observing current Information Sharing
Notification protocols
Share within guidelines
some guidance

WG2 places emphasis on information exchange, not information transfer
peer-to-peer organisation, with flows of information that are balanced in terms of giving and receiving.
All members actively share as well as listening. In this regard, the recommended WG2 Information sharing platform can be distinguished from CERTs/CSIRTs, which tend to issue greater quantities of authoritative information than they receive.

Trust is personal – it grows slowly between people. Therefore meetings take place face-to-face, and representatives must attend. They cannot send a substitute as a stranger turning up at a meeting would inhibit the sharing of sensitive information.

Sharing of sensitive information is done using standard mechanisms (e.g. Traffic Light Protocol).
Disseminate of information could also be done through protected extranets usually managed by the government.
As trust within the group grows, members develop informal links via telephone and/or email.

As trust within the group grows, members develop informal links via telephone and email;

Members must realise this is a personal appointment; no substitutes are allowed to attend, and they understand the obligation to give the same weight of information as they receive;
Members are expected to give the same level of information as they receive, under conditions of confidentiality.

3.1 Scope

All hazard, cyber included
Information sharing partners: Technical, operational, political-strategic

3.2 Guidance on Privacy and Trust with Information Sharing

To maintain trust a sharing platform need to be very sensitive in approaching commercially sensitive issues such as quality of service and availability, which are seen by some private sector members as having significant competitive advantage. Forcing detailed disclosure of such information, for instance, could seriously damage relationships, and in some countries may be considered illegal if industry members could be considered setting up a cartel.

3.3 Shared information

Focus on relevant value add services
It may sound obvious that the information exchanged must be relevant to the members and add value, but observations have been made where information has been introduced which has little value. This can easily happen when the threat is low with few incidents to

discuss but it is thought better to have shorter meetings than fill the meeting with low value information. To prevent this happening it is good practice for a sharing platform to state clearly the scope and criteria of the services it provides:

1. It must concern and support a member, the whole sector or all parties in their mission to strengthen their information security process.
2. The information must have an added value. (i.e. not available somewhere else).

Information inputs and outputs
Information, physical and personnel security information is collected from a wide range of sources.
What information is shared? Any type of information which is deemed interesting and valuable in order to support increasing the sharing platform members' information security, is collected, disseminated and shared;

Information that might usefully be shared would include:

- Incidents,
- Risks,
- Threats, analysis on threats
- Attacks,
- counter measures,
- Response,
- Impact and vulnerabilities,
- Cooperation,
- Product technical vulnerabilities and risks,
- Protocol vulnerabilities,
- Network intrusion information,
- Probing attacks and network configuration issues within standards
- Advisory support in implementing protective measures;
- Alert service on attacks and incidents
- Information on cyber security, incidents, security measures,
- Information on contingency planning, on single point of failures, dependencies, crisis management arrangements, exercises
- Best practices, Peer good practice;
- Discussions around good practices and recent trends and developments;

How is information validated?

3.3.1 Example for Incident reporting

Content taken from [ENISA 2013-1]

Three types of incident reporting:
1) National incident reporting from providers to NRAs,
2) Ad-hoc incident reporting between NRAs and ENISA, and
3) Annual summary reporting from NRAs to the EC and ENISA.

The different types of reporting are shown in Figure 1.

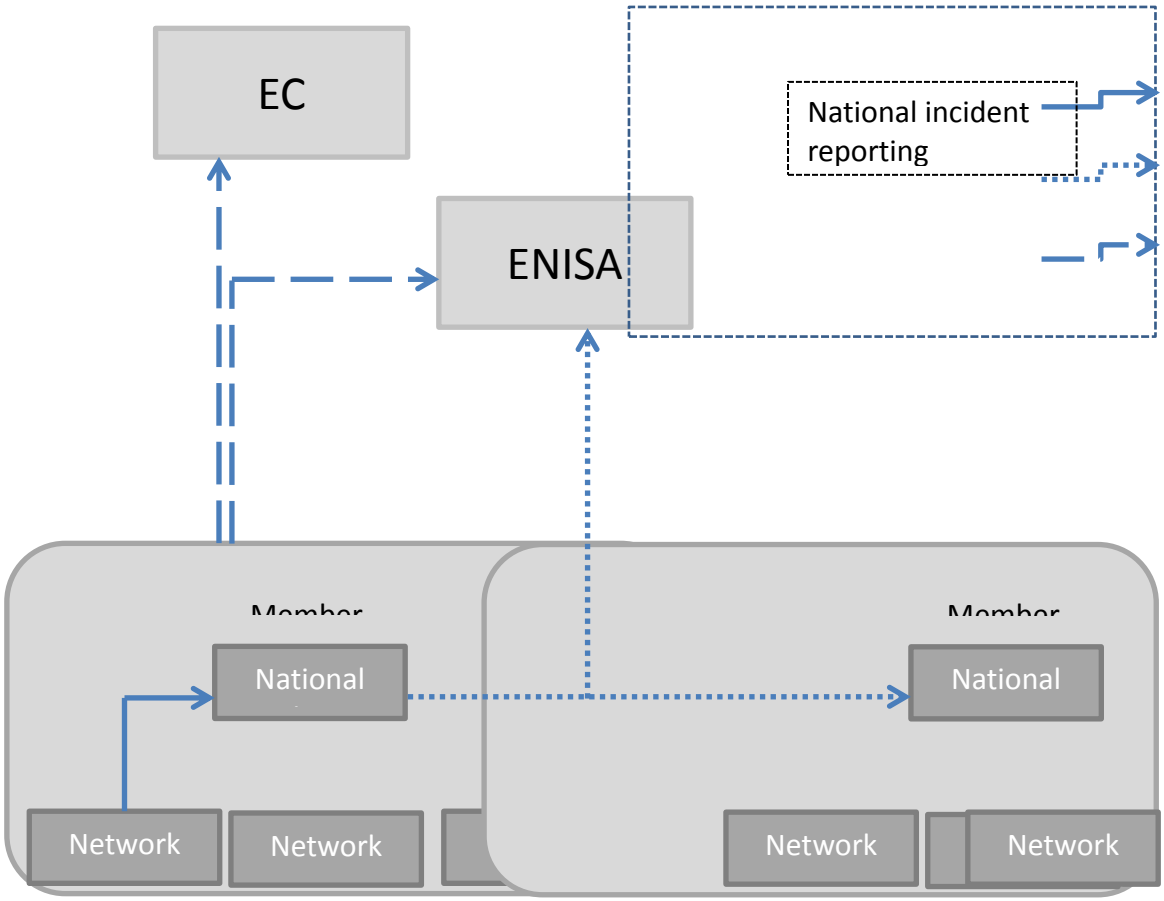

Figure 1. Three types of incident reporting

Note that it is at the discretion of the NRA to determine what is significant. This ultimately depends on national circumstances. For example, a security incident affecting just a small number of users in a specific area could already be considered significant by an NRA.

A security incident can have different types of impact on the operation of services.

- Impact on the continuity of supply of services.
- Impact on the security of users and interconnected networks

National user base

To allow for aggregation at an EU level (one of the goals of annual summary reporting) NRAs should provide ENISA and the EC with estimates of the total number of users of each service in their country. NRAs may (optionally) use the following metrics as estimates:

Thresholds:

The threshold for annual summary reporting is based on the duration and the number of users of a service affected as a percentage of the national user base of the service.

User minutes

3.4 Critical Success Factors

"Other critical success factors identified included:
● Establishing effective and appropriately secure communication mechanisms, such as regular meetings and secure Web sites;
● Obtaining the support of senior managers at member organisations regarding the sharing of potentially sensitive member information and the commitment of resources;
● Ensuring organisational leadership continuity.
● Providing identifiable membership benefits, such as current information about threats, vulnerabilities, and incidents. Without such benefits, according to the representatives we met with, members would not continue participating."
(United States Government Accountability Office 21)

for the trust to be complete i.e. to trust industry and every industry member had to trust the rest.

4 Service and Incentives

Grudzien/Semple/ENISA (no subgroup)
What services and incentives should be offered?'

[Recommendation 27]
PPPs should create a mechanism for members to influence the services provided which meets their needs. This could be a regular agenda item as well as agreeing in advance a yearly work programme.

[Recommendation 28]
To deliver value added activities, PPPs should ensure that the services provided address the problems identified and align with the agreed scope focus.

[Recommendation 29]
It is important for a PPP to define the benefits to members, both services and incentives, explicitly. This will not only sustain the interest of members but also support them in securing the support of their management.

[Recommendation 30]
PPPs should clearly leverage the skills, experience and organisational positions of the existing members to provide an incentive for new members.

[Recommendation 31]
All members of the partnership, including the public sector members, need to actively contribute information, services or support that is of relevant value to the membership. Where members fail to make a positive contribution action should be taken by the membership to resolve the situation.

[Observation 21]

The range of services changes and grows over time, led by the needs of the membership and the lessons learned. For example Good Practice Guides are often produced after the PPP has addressed the corresponding problem.

[Observation 22]
Creative approaches have utilized services to gain membership interest, for example offering cheap or free training to candidate members. The training was of genuine value but also enabled the attendees to understand the importance and value of membership.

[Observation 23]
Not all members need to contribute the same types of value. Some may offer technical knowledge while others funding. Some may offer intelligence while others research and analysis.

4.1 Services

Research/Analysis ● Crisis Management
● Good Practice Guides ● Resilience Planning
● Information Exchange ● Emergency Planning
● Rapid Response/ Early Warning ● Security Audit
● Exercises ● Benchmarking
● Awareness Raising ● Supervisory/ Co-ordination
● Technical Evaluation ● Statistics
● Defining Standards ● Archiving
● Help Desk/ Triage ● Strategic Planning
● Risk Analysis

4.2 Incentives

Incentives can be more than money. Participation reduces risks so an incentive could be part of liability protection or to reduce premiums in cyber-risk insurance.

Costs of prevention versus costs of recovery could be presented.

Sharing platform focus on electronic/physical attacks, malfunctions of systems, interdependencies with other sectors and natural disasters
Sharing platform provide commercial benefits to its members

ENISAs work on Incentives and Barriers.

- operational benefit from cost-savings and time to react to serious failures
- Sharing a Critical Problem
- Access to Privileged Information from government
- Economic Incentives above cost savings
- Reputational Benefits, both from a personal and organisational viewpoint
- Access to advice & Knowledge not available elsewhere

- possibilities to influence government policy and avoid the introduction of misplaced regulation
- Industry is able to speak as one voice
- Co-operative support during a crisis

5 Protocols

Semple
Conduct of sharing which links into the question of trust and privacy, actual protocols of sharing, governments

5.1 Communication Rules

An agreed distribution policy has been shown to help build trust. The Traffic Light Protocol was found to be used widely where Red information is the most sensitive. Other good practice used by some CIP-Programs is the 'Chatham House Rule'.

5.1.1 Traffic Light Protocol (TLP)

[ENISA 2009-1] Appendix C

5.1.2 Chatham House Rule

[ENISA 2009-1] Appendix D

6 Recommendations from WG2

- PPP Cross Sector, European wide, deed of confidentiality
- WG2 recommended Information Exchange platform is designed to encourage mutual trust
- Addressing the bigger picture for the general good of the industry
- For discussion: The agenda and time frame of WG2 concentrates on longer term prevention of major incidents and emergencies rather than real time 'fire-fighting'.
- For discussion: Keeping membership small fosters trust.
- Sharing platform members are senior experts with relevant skills
- Sharing platform members are senior experts that have management authority to share sensitive information with their peers.
- They normally have a strong background in security and resilience and could mobilise resources wherever change is needed to address vulnerabilities, risks and threats (Chief Security officer or equivalent).
- The members meet regularly and face-to-face (usually 4-6 times per year) to share sensitive information.
- No participation fees for members
- Stakeholders taking part consider it cost effective but a participation fee could be seen as a barrier, especially during the early life of the Sharing platform.

6.1 Sharing Platform

6.2 Notification Process

6.3 Next Steps

7 Appendix

7.1 Sources

ENISA 2009-1	Good Practice Guide - Network Security Information Exchanges, ENISA, June 2009.
ENISA 2011-1	Cooperative Models for Effective Public Private Partnerships - Desktop Research Report, ENISA, 2011.
ENISA 2011-2	Cooperative Models for Effective Public Private Partnerships - Good Practice Guide, ENISA, 2011.
ENISA 2010-1	Incentives and Challenges for Information Sharing in the Context of Network, ENISA, 2010.
ENISA 2013-1	Technical Guideline on Incident Reporting - Technical guidance on the incident reporting in Article 13a, ENISA, Version 2.0, January 2013.
UPK-1	German CIIP (UP KRITIS)