EP3R 2013 – Position Paper

Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS)

October 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This Position Paper was prepared and developed by the following Experts:

- Manuel Barros, Anacom
- Fabio Bisogni, Formit
- Peter Burnett, Quarter House Ltd
- Genseric Cantournet, Telecom Italia
- Simona Cavallini, Formit
- John Harrisson, LandITd
- David Pollington, Microsoft
- David Sutton, Tacit.Tel
- Simon Van Merkom, Ministry of Economic Affairs , Agriculture and Innovation
- Reiner Wyphol, BnetZa – Bundesnetzagentur

Lionel Dupré, ENISA is the editor of this report.

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

Executive Summary

Within the European Public Private Partnership for Resilience EP3R Task Forces (TFs) the Information sharing TF not only had a research purpose, but also aimed to lay the groundwork and define the requirements and topics of an information sharing approach. This approach aimed to deliver trusted relationships among participants of groups within EP3R and may also be a reference point for comparable initiatives.

The proposed approach is based on trusted relationships in groups sharing information in a remote mode. According to the new ISO/IEC 27010:2012 standard[1], a key component of trusted information sharing is a 'supporting entity', defined as *"A trusted independent entity appointed by the information sharing community to organise and support their activities, for example, by providing a source anonymisation service"*

For this reason, the Task Force defines both management/process requirements and functional requirements of a potential online tool. Requirements that generally apply to communities engaging in trusted information sharing groups were selected according to the EP3R needs. The Task Force however ensured that the requirements wherever trusted information sharing is needed, e.g. for the work of the Working Groups of the NIS Platform.

In order to better tailor the generally applied requirements to EP3R, the Task Force also put a special effort into understanding what information needs to be shared, what sensitivity levels are involved and the professional profiles appropriate to participation in the sharing. A particular focus of this investigation was on topics of interest not only for the EP3R but also for the other communities dealing with security and resilience of ICT and protection of Critical Information Infrastructure (CIIs) in general.

It became evident during this work that it was crucial to identify a suitable 'supporting entity' to host and manage an online trusted information sharing system. The Task Force members were unanimous that ENISA was the most obvious and most suitable choice for this. It also became clear that ENISA's remit might cause difficulties with adopting such a role, and that a suitable legal basis would be necessary to safeguard the privacy of any information shared through such a system. Nonetheless the TF felt that this was the best way forward, as no other existing entity was considered to be so suitable.

The key recommendations of this report are:

- To establish a pilot based on the Management and Functional Requirements listed in this document which usage will allow a more structured Information Sharing mechanism;
- To designate a neutral party who will host and operate this platform. The Task Force estimated that ENISA could be an option to investigate;
- To encourage the use of these requirements in other projects and communities.

[1] **First few pages of ISO/IEC 27010** http://webstore.iec.ch/preview/info_isoiec27010%7Bed1.0%7Den.pdf

Contents

1 Introduction

In 2007 the European Commission (Information Society and Media Directorate-General) published the results of its commissioned ARECI (Availability and Robustness of Electronic Communications Infrastructures) study; this seminal report had a key recommendation on trusted sharing:

"Member States and the Private Sector should establish formal means for sharing information that can improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe".

At the June 2012 EP3R workshop, members suggested that the time is right to trial an electronic system specifically designed to facilitate Trusted Information Sharing amongst members of EP3R when face-to-face meetings are not viable. ENISA suggested that a small Task force should be created to make recommendations for a system, which would initially build on the existing (but limited) amount of trust between certain members who are familiar with each other, but will allow for the gradual extension of the group to new members. In this way, it will be possible to develop multiple Trusted Information Sharing groups within the EP3R membership, overlapping where appropriate. It is hoped that this mechanism will improve the commitment and productivity of EP3R members, and should be extensible beyond EP3R to related groups and topics**.**

1.1 Goal

The task force was requested to consider a number requirements that would allow the gradual building of Trusted Information Sharing at Pan-European level. They are presented below, and organised between Management / Process requirements (as Principles), and Functional Requirements, should a technical platform be implemented one day to reduce the need for Face to Face meetings.

Information sharing was taken by the Task Force not as an end in itself, but initially as a means to build trusted relationships among EP3R participants.

The principles proposed are basic and obvious, but raising them within such a platform establishes a de-facto standard for existing and future pan-European partnerships.

1.2 Target audience

This document not only addersses the needs of any PPP which needs to implement a remote (i.e. non face to face) trusted information sharing mechanism, but any other community with similar needs. A list of possible customer communities is presented later in the document.

1.3 Structure of this document

This document first provides an analysis of the situation which was within EP3R, and how the need of information sharing arose as a horizontal topic. Since such an analysis would be useful in other contexts, the working group gradually expanded their considerations beyond the initial work objectives by analysing how it could benefit to other communities also.

The document then provides a number of formal Management and Process requirements, complemented by a set of Functional requirements.

Those requirements altogether form the foundations for a sound Trusted Information Sharing Platform.

2 Identifying the Needs

2.1 Information Sharing as a means, not a Purpose

Several references and mentions were made during the analysis phase about the other work developments made in this area (See References at the end of this document).

This report actually uses many of the recommendations and issues contained in ENISA's Good Practice Guide on Information Sharing[2] and instantiates many basic principles into actionable ones.

The Task Force stresses that while Information Sharing is a foundation for any Partnership, it is not a goal: the purpose is to implement applied Information Sharing on many topics, and the other EP3R Position Papers actually built up on the assumption that Information Sharing mechanism would be ready in 2014 to complement face-to-face meetings.

Such a platform was also seen as a condition sine qua non for the sharing of more and more useful information. The value of such platform could even drive more people to consider the supported PPP as a valuable service, solely because of the trust building features associated.

2.2 Topics and Communities

Although there are many common principles and requirements for Trusted Information Sharing, as described in ISO/IEC 27010:2012, it is important to understand, from an EP3R perspective, what information needs to be shared, what the sensitivity levels of the information that need to be shared are (if we assume we should not share highly sensitive information) and who will participate in the sharing. This will help in the creation and validation of the requirements for Trusted Information Sharing.

This section identifies specific Topics and Communities for sharing within any CIIP opportunities at a European level. This includes suggested future topics and communities, identified by the members of the Task Force.

2.2.1 Initial Topics and Communities

The EP3R (to mid-2012) was divided into four Working Groups (WGs). This structure has encountered problems where some members have interests in several areas but are unable to engage in parallel workshops based on WG lines. The structure has been revised, and a less rigid format has been adopted, but conflicts of interest will still occur. It is believed that an electronic trusted group model will significantly mitigate this. It can also help to address the fundamental issues affecting all WGs. These include inconsistent and fluctuating attendance (due to availability) at teleconferences and workshops that affected the opportunity to build stable professional and personal relationship. As a consequence this led to the inhibition to share sensitive information due to the presence of untrusted and unknown members in a teleconference or workshop. This has made it very difficult to build trust due to the high turnover of the participants to face to face and even telephone meetings.

[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

The membership of virtual Task Forces can be tightly controlled, and the dissemination of any sensitive information can be completely controlled by its author, thus helping to build trust.

The following eight headings help categorise the experience of the former EP3R.

Primary objective of sharing: The objectives of the three initial groups were specified by the Commission with the expectation that the output would add value to the membership as well as feed into the European Commission strategy and regulatory policy. These groups have run over several years as it has been difficult for members to agree the true objectives partly because it has been difficult to engage with a consistent community with only a few meetings a year.

Community: The former EP3R community included public and private sector, telecom operators and ISPs, hardware/software vendors, regulators and consultants. Consistent representation from this diverse community has been difficult at times partly because of conflicts with diaries for meetings. Diverse representation has also made it difficult to focus on the real issues and deliver useful outputs.

Multiple Sharing communities: For most of the life of the initial groups, face to face meetings have been held in parallel sessions, which make it difficult for an individual to be involved in more than one WG. Plenary sessions allow communication of findings but it is still not easy for those not in the WG to make a contribution.

Supporting entity: Moderators for each group have been introduced during the last two years, which has helped bring better focus on the activities. These moderators have helped to build trust within each group.

Membership governance and control: In EP3R, group membership was open to all, with no control over how information is shared at meetings other than a verbal agreement in some meetings to adopt the 'Chatham House Rules'. There is a closed online portal for members but anyone who attends meetings is given a login identity and password for access.

Information shared: Of the ten types of information shared that are listed in Annex B, five have been observed in existing WGs: Advice; Analysis; Other; Peer good practice and some aspects of Contingency planning.

Confidentiality and Anonymisation: This is not possible with the current open community and consequently the output of the WGs will be at a highly generic level.

Comment: In 2011, ENISA changed the structure of EP3R and move away from large long-term groups to small rapid action Task Forces with clearer objectives and addressing many of the issues described in the above headings.

2.2.2 Incentive for extension to other topics

Since Information Sharing was the major concern in the recent developments within several communities, the idea of the Task Force was to derive a list of requirements possibly applicable in other areas too.

2.2.3 Suggested Future Topics and Communities

2.2.3.1 Article 13a

ENISA recently implemented a web-based tool for the reporting of Incidents in the context of the Article 13a obligation.

It relates closely to other recommendations raised in the Task Force on Incident Management. Its purpose is to share solely relevant internal emergency procedures, contact details, and incident detection specifications among CII operators to support the other Management Requirements.

Primary objective of sharing: This community would address the compliance needs of National Regulatory Authorities (NRAs), operators and service providers working within the scope of Article 13a.of directive 2002/21/EC.

Sharing of findings on practical matters regarding "developing" measures, application of measures; enforcement experiences; sharing of statistics on incidents.

Community: This would be a closed community of telecom operators and regulators from Member States (MS) who have a duty of compliance with Article 13a.

Multiple Sharing communities: Some of these already exist at the National and European levels.

Supporting entity: These are appointed contacts at the National level, Regulators as well as operators (which could be operator associations or similar); ENISA at the European level.

Membership governance and control: These functions are key to meeting the primary objective. A possible option is that ENISA takes care of this as it is more neutral than a Member State or operator - a similar process is in use for the ENISA portal.

Information shared: Of the ten types of information shared in Annex B, seven are thought to be relevant to this topic and community: Experience, Advice; Analysis; Other; Peer good practice, Incidents and vulnerabilities and some aspects of Contingency planning.

Confidentiality and Anonymisation: These features are key to meeting the primary objective. ENISA as a central focal point could anonymise information or data and store it in a secure way. Application of a formal information classification scheme might not work because operators should then need to have employees screened up to a specified clearance level, which could exclude some members . The Traffic Light Protocol (TLP) might be a way forward, but it would be necessary to identify a mechanism to ensure that the confidentiality of TLP-marked information was not compromised through Freedom of Information (FoI) provisions. Anonymisation of the source is done by the National Regulatory Authority (NRA) when sharing at the European level.

Comment: Much of the information relating to article 13a in its raw state is likely to be sensitive and therefore must be protected accordingly. At the European level there is less concern about naming and shaming, as the NRA protects the source at the national level by providing anonymity. There is a good level of trust between NRAs across member states with transparency preferred amongst users of any platform.

2.2.3.2 'Black Swan' risks

Primary objective of sharing: This community would address the risks associated with high impact low probability events, also known as 'Black Swan' events, which relate to the security and resilience of the telecommunications network at the European level.

Community: This consists of both Public and Private parties who are closely related to the "scope" and "environment" of the risk; so this could lead to several communities each related to a certain Black Swan. Security directors for the private sector and officials for the Public; CIIP owners and service providers, and National Competent Authorities.

Multiple Sharing communities: Potentially with other sector based communities such as professional Information Security associations e.g. ASIS[3], ISSA[4] etc.

Supporting entity: Each Black Swan could be coordinated by either the party which is likely to be most involved when the risk comes to fruition, or the party which has most expertise about the risk. Appointed contacts in either of the two parties above, at the National level; ENISA at the European level.

Membership governance and control: High level supplied credentials are needed; existing members will introduce a new member. This could be modeled on a University Scientific Board, such as the one created in Italy about Economic Intelligence.

Information shared: Of the ten types of information shared in Annex B, all ten are deemed relevant to this topic and community: Experience, Advice; Alerts; Analysis; Contingency planning; Warnings; Other; Peer good practice, Incidents and vulnerabilities and Physical and Personnel.

Confidentiality and Anonymisation: High confidentiality is required. The need for anonymity may be less because there is only a small group dedicated to each Black Swan, and it is in the interest of that specific group that the risk/threat/problem of "their" Black Swan is solved without much (media/parliamentary) attention. Another view is that it is not necessary because of the low likelihood which appears as unrealistic.

Comment: This is an important topic, particularly because it is not evident that it is being fully addressed elsewhere. Black Swans are not a specific category to be dealt with apart but the extreme part of the spectrum/continuum of threats.

2.2.3.3 Exercises

Primary objective of sharing: Share experience and knowledge on exercises (private only, or private and public) , include scenarios ; also private parties which are member of the community might coordinate who of the private parties will participate in which exercise as player or as a simulation cell.

[3] *ASIS: ASIS International (American Society for Industrial Security),http://www.asisonline.org/*

[4] *ISSA: Information Systems Security Association, https://www.issa.org/*

Community: Private parties interested in participation in exercises.

Multiple Sharing communities: Exist at EU/ENISA level.

Supporting entity: ENISA is already acting in a coordinating role regarding exercises.

Membership governance and control: Members have to actively participate in exercises, not just sit and listen.

Information shared: Of the ten types of information shared in Annex B, Contingency planning is deemed the most relevant to this topic and community.

Confidentiality and Anonymisation: Less important; some applicability to exercise results when a player has found interesting issues to improve, or lessons might be critical or embarrassing.

2.2.3.4 Critical Information Infrastructure Protection (**CIIP)**

Primary objective of sharing: Share experience and knowledge on protecting the Critical Information Infrastructure (CII), especially at the European level; should be supporting multi-member state or even EU-wide activities on CIIP such as risk assessments, impact analysis, good practices on protective measures, etc., in addition to and cooperating with national activities/projects.

Community: Private and public parties who play or should play a role in protecting the CII, being prevention, preparation or response or alike; also maybe EU-wide associations representing a particular market sector (an example is electricity: national companies should be members and also their EU associations because those associations are carrying out CIIP activities too).

Multiple Sharing communities: Exist at EU/ENISA level for some subjects; exists at national levels.

Supporting entity: Could be ENISA because of EU wide contacts and overviews, of experience based on art13a incidents and of general expertise from ENISA studies.

Membership governance and control: Based on stakeholder analysis for a certain CII (CII provider as well as "CII user")

Information shared: Of the ten types of information shared in Annex B, all ten are thought to be relevant to this topic and community: Experience, Advice; Alerts; Analysis; Contingency planning; Warnings; Other; Peer good practice, Incidents and vulnerabilities and Physical and Personnel.

Confidentiality and Anonymisation: Same approach as national level, based on the combination of the seriousness of the risk / criticality of the CII different confidence levels/procedures should be used.

Comment: None

2.2.3.5 Cybersecurity / Crime information exchange

Primary objective of sharing: EU equivalent of UK NISCC/CPNI and NL CPNI.nl.

Community: Public parties active in research on cybercrime/cybersecurity and in fighting cybercrime and private parties who have to implement the operational measures to fight cybercrime or who provide services/infrastructure which is used by cybercriminals.

Multiple Sharing communities: Exists at the national level in some Member States.

Supporting entity: Could be ENISA because of EU wide contacts and overviews, of experience based on art13a incidents and of general expertise from ENISA studies.

Membership governance and control: Based on stakeholder analysis by national authorities include "credentials".

Information shared: Of the ten types of information shared in Annex B, seven are deemed relevant to this topic and community: Experience, Advice; Analysis; Other; Peer good practice, Incidents and vulnerabilities and Physical and Personnel.

Confidentiality and Anonymisation: Same approach as national level, (CPNI-like approach).

3 Implementing an Online Trusted Information Sharing System

3.1 Translating into Formal Requirements

3.1.1 Purpose

At the early stages of the Task Force's discussions, a number of concerns were raised by participants which led to consider the problem from a Functional Analyst's standpoint. It became progressively obvious that the position paper produced by the Task Force would take the form of a list of requirements.

3.1.2 Benefits

Listing requirements was a rapid way of establishing the features and rules that should be imposed on a proper Trusted Information Sharing platform. Other methodologies would have taken considerably longer, and possibly not left enough flexibility of implementation in the end.

3.1.3 Management/Process Requirements

The following list of requirements has been found to generally apply to communities engaging in Trusted Information Sharing.

M/PR1	The primary objectives for sharing information within the group should be identified and published. These objectives should emphasise the benefits of sharing in order to promote participation.
M/PR2	The type of information that should be shared in order to achieve the objectives should be identified.
M/PR3	Existing sharing standards should be identified and used where possible in order to speed agreement and implementation.
M/PR4	A procedure for anonymising shared information is required.
M/PR5	An agreement is required defining how the information shared can be used by the recipients. (For example using the Traffic Light Protocol).
M/PR6	In order to support anonymisation, and to manage membership and chairmanship of the trusted sharing community, a trusted third party may be required.
M/PR7	An agreement will be required to establish the ownership of shared information, and the rights of contributors to control the sharing of supplied information.
M/PR8	It will be necessary to define the membership criteria for a sharing community. It may be necessary to implement more than one sharing community.
M/PR9	For each sharing community the method of identifying potential members should be established, along with the processes for joining and leaving.
M/PR10	Technical controls should be employed that are appropriate to the sensitivity of the information exchanged, for example, encryption may be required if the information must not be revealed outside the sharing community.
M/PR11	Where information is anonymously contributed, it must be possible for the sharing community to be given confidence in the quality and source of the information, while

	maintaining the anonymity of the originator.
M/PR12	Guidance should be provided to members of the EP3R sharing community, defining their responsibilities when handling shared data.
M/PR13	A commitment to sharing is required in order to remain a member of a particular community.
M/PR14	A mechanism for appropriate legal measures such as NDAs may be required to protect the interests of those sharing some information.
M/PR15	A mechanism for extending trust between trusted sharing communities must take account of each communities trust requirements.
M/PR16	A mechanism should exist for optional association so that groups with related interests can be linked together for information exchange.
M/PR17	A mechanism should exist to protect the identity of sharing group members when required.

3.1.4 Purpose

In order to support the Management/Process Requirements identified above, a technical solution for Trusted Information Sharing must fulfil the following functional requirements. Each requirement in this section is cross-referenced to the Management/Process requirements where possible.

3.1.5 Functional Requirements

FR1	The solution must facilitate the automated flow of information between and among public and private sector entities in a timely, consistent, and predictable manner within a trusted environment, where information is received, disseminated, analysed, and protected appropriately	[M/PR1, M/PR2, M/PR15, M/PR16, M/PR17]
FR2	The solution must establish clear roles and responsibilities to help all members know how they fit into the information sharing landscape	[M/PR5, M/PR12]
FR3	The solution must be scalable both in terms of accommodating several potentially overlapping sharing communities, incorporating additional users/contributors from any geographical location, and in terms of the format and content of information to be shared	[M/PR2, M/PR8, M/PR9, M/PR15]
FR4	The solution must include a highly intuitive interface, be simple to use and to navigate through and be sufficiently flexible in its user interface to be personalized to suit individual users or user groups	[M/PR12]
FR5	The solution should be able to provide metrics to determine who are the major contributors and consumers of shared information	[M/PR13]
FR6	The solution must allow users to search for and retrieve contact details for authorized users, where permitted	[M/PR6, M/PR7, M/PR8, M/PR17]
FR7	The solution must specifically support the anonymisation of shared information, by providing a sharing workflow that involves a trusted third party or supporting entity	[M/PR4, M/PR6, M/PR11]
FR8	The solution must provide appropriate operational and technical capabilities to protect and secure data to ensure the integrity, availability and confidentiality of all information	[M/PR10]
FR9	The solution should allow originators of information to assign a degree of trust in the data and information they input	[M/PR5, M/PR12, M/PR13]
FR10	The solution must ensure that all users will be uniquely identified and authenticated before being given access	[M/PR9, M/PR10]
FR11	The solution must ensure that all information is appropriately protected from unauthorized access, including at system administration level	[M/PR10, M/PR17]
FR12	The solution should allow for the examination of audit data (logs) via an auditing mechanism that can determine whether actions performed by users meet the policy requirements of membership and can hold users accountable for their actions by recording what they do	[M/PR12, M/PR13]
FR13	The solution must allow for the archiving of data to match the expected life-cycle of the system, with full backup and restore facilities being	[General]

	provided	
FR14	The solution should allow for a graduated uptake of collaboration, including a set of basic features (for quick uptake by users) and more advanced capabilities for users more experienced with secure collaboration	[M/PR1, M/PR2, M/PR3]
FR15	If the membership is split into multiple sharing communities, the solution should allow users of one community to be able to share information with members of others, either through a trusted moderator or directly	[M/PR8, M/PR15]
FR16	The system should be universally accessible from all major web browsers, via the Internet	[General]

4 Observations and Next Steps

During the creation and review of this requirements document for Trusted Information Sharing, a number of important observations and recommendations were made by Task Force members, which are listed in this section. [References to other parts of the document are shown in square parenthesis]

a) Effective trusted information sharing across organisations, companies, and countries will depend on the availability of a system to enable sharing and that the participants have trust in the hosting of the system. [FR8, FR11];

b) There should be an analysis of available information sharing systems against the requirements contained within this document. The Commission has a few trusted communication systems available, e.g. CIWIN implemented under EPCIP and the ENISA LISTSERV and Resilience Portal which should be included in the analysis. [Annex A, Deliverable 2];

c) Careful consideration should be given to the inclusion of regulators in trusted sharing groups to balance the benefits with possible conflicts of interest. [M/PR8]

d) ENISA is suggested as the 'supporting entity' – see 3.1.They have already gained some experience; they have contacts in public and private sector. Organizing by a third party or an administration or operator could lead to lack of confidence or maybe activities with good intentions but which lie outside the scope of the structure;

e) In addition to a trusted information sharing system (see a) there should be consideration given to the provision of a trusted voice, video and application collaboration mechanism;

f) There should be a trial of this system to prove the benefits and refine the requirements using topic(s) identified in section 5.2;

g) Standards should be investigated and applied where appropriate (e.g. 270## series and possibly 28001); membership and governance rules will be needed as a foundation and framework to make this happen and it is recommended that ISO/IEC 27010:2012 is studied in detail to produce a compliance statement on its suitability. Other standards should also be studied such as ISO/IEC DIS 29147 – Security techniques - Vulnerability disclosure to avoid any potential conflicts of interest.

h) The trusted information system is not intended to handle national or EU classified information;

i) The application of this trusted information system can be extended outside of EP3R and could include CERTs. [Annex A- Scope of Task Force];

j) A 'terms of reference' document should be created to bring together the management and process requirements for each trusted sharing community addressing specific topics. This may include legal protection provision for the information being shared;

k) The trusted information system is not intended to be used for real time incident handling;

l) The CIIP topic 5.2.4 should be broken down into sub-topics suitable to trusted information sharing groups of appropriate size homogeneity;

m) There are significant reservations about the inclusion of cyber-crime within the scope of the trusted information sharing system, which is not intended to hold sensitive cyber-crime

information. This document has not specifically addressed the requirements of the law enforcement community related to cyber-crime;

n) In the consideration of ISO/IEC 27010:2012 principles, consideration should be given to the emerging draft standard ISO/IEC DIS 29147 – Security techniques - Vulnerability Disclosure.

Recommendations

EP3R-TF-TIS 201301 – ENISA should Implement a System Trial using the Functional and Management Requirements defined in this Position Paper

As described in this Position Paper, the EP3R Task Force on Trusted Information Sharing evaluated a number of Functional and Management Requirements which form altogether a consistent Functional Analysis for an Online Trusted Information Sharing Platform.

The Taskforce recommends the establishment of a Trial of such platform, and evaluate how a wider implementation could be done at a later stage. The purpose of such trial would be threefold:

- Assess technical implementation feasibility;
- Provide a usable pilot and assess usability of such pan European mechanism;
- Assess Participants buy-in and how trust was established between them.

The Task Force identified ENISA as a 'Supporting Entity', notion which is defined in the ISO Standard 27010:2012, and therefore recommends that ENISA implements this pilot and runs this trial.

EP3R-TF-TIS 201302 – PPPs should consider the adoption of these requirements for Online Trusted Information Sharing

These requirements were initially drafted based on the observations made in the late EP3R, but also on the PPPs studied during the study on Cooperative Models for Effective Public Private Partnerships[5]. Those requirements have been made generic enough to be easily adapted to different situations, and therefore the Task Force recommends that European PPPs implement these requirements also for any new Trusted Information Sharing, or adopt a platform which presents these characteristics.

EP3R-TF-TIS 201303 – Trusted Information Sharing for Incident Preparedness, Early Warning, Management and Post-Mortem

Discussions in the EP3R Task Force on Incident Management raised the needs for establishing Trusted Information Sharing to implement the systematic exchange of Incident Preparedness data, such as contact data, roles and responsibility, Emergency procedures, etc.

The Task Force on Trusted Information sharing again recommends that the Requirements listed in this paper are implemented on the platform used.

[5] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps

Conclusions

A key component of trusted information sharing is identified in the ISO/IEC 27010:2012 standard as being the need for a 'supporting entity', defined as:

"A trusted independent entity appointed by the information sharing community to organise and support their activities, for example, by providing a source anonymisation service"

The Task Force members recommend that ENISA is the supporting entity and operates such a platform.

An effective trusted information sharing mechanism will be dependent upon the right people in the right roles with the right empowerment to represent their organisations and all within a predefined and authorised exchange process. Membership and Governance rules will be needed as a foundation and framework to make this happen and it is recommended that ISO/IEC 27010:2012 is studied in detail to produce a compliance statement on its suitability. Other standards should also be studied such as ISO/IEC DIS 29147 – Security techniques - Vulnerability disclosure to avoid any potential conflicts of interest.

To move the objectives of the Task Force forward the suggestion to hold a trial (Recommendation EP3R-TF-TIS 201301) should be actively pursued as this will help determine the true requirements. This trial should be conducted as part of the requirements phase of the Task Force and is not dependent on the other activities previously.

References

- ISO/IEC 27010: http://webstore.iec.ch/preview/info_isoiec27010%7Bed1.0%7Den.pdf
- Trusted Information Sharing: Why would I tell you ? Perceived Influences for Disclosure Decisions by Senior Professionals: in Inter Organisation Sharing Forums http://www.warp.gov.uk/downloads/Why-would-I-tell-you.pdf
- Tools to build Trust: http://www.warp.gov.uk/building-trust.html .
- IAAC: A review of Information Sharing: http://www.warp.gov.uk/downloads/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.pdf
- ASIS: ASIS International (American Society for Industrial Security), http://www.asisonline.org/
- ISSA: Information Systems Security Association, https://www.issa.org/

Related ENISA papers

- Good Practice Guide on Information Sharing: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide
- Cooperative Models for Effective Public Private Partnerships: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps

Annex A: Tasking Brief for EP3R TF1 - Trusted Information Sharing Mechanisms

A.1 Background

It has been recognised for some time that Public-Private Sector Partnerships need to create an environment for trusted information sharing if they are to add real value to their membership and improve CIIP. ENISA has produced a number of good practice guides on how to create and run these co-operative environments[6]. EP3R is no exception, and at the Brussels workshop of 6 June 2012, a number of participants requested action to create this environment and start trusted information sharing. The purpose of this document is to set out the requirements for an Information Sharing Task Force that will move this proposal forward.

This Task Force will create a proposal for a practical application of trusted information sharing mechanisms for use by EP3R.

A.2 Scope of task force

The task force will:

- Address the needs of EP3R participants for trusted information sharing in order to deliver the mission of EP3R both now and in the future.
- Take account of existing initiatives in the field of Information Sharing
- Take account of possible future directions for EP3R and its relationship with EFMS.
- Look at the requirements for effective sharing of information by EP3R participants, including the need for confidentiality and anonymity while at the same time addressing the need to make EP3R open and transparent. Striking the right balance between these two aspects is seen as a crucial element of the scope.
- Take account of CIIP trusted sharing opportunities outside of EP3R, in any recommendations made.

A.3 Approach of task force

The task force will include EP3R moderators, and will make use of the extensive experience in trusted information sharing mechanisms of other members of EP3R. They will engage with a carefully selected group of active EP3R participants from both a public and private sector background who are known to share common issues with a strong interest in trusted information sharing.

A.4 Deliverables

1. A list of collective requirements for trusted information sharing in EP3R will be drawn up by the task force, including potential sharing communities and associated topics for trusted sharing.
2. Existing trusted information sharing mechanisms would be studied and documented.
3. The resulting list of mechanisms will be compared to the collective requirements of the task force members to ensure that any proposal is requirements-led.
4. A proposal with justifications will be made, recommending the most appropriate sharing mechanism. In this context, the 'sharing mechanism' will address the trust framework of

6 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps?searchterm=Cooperative+model

membership, governance, platform and standards for sharing (e.g. ISO 27010:2012), suitable for the wide range of existing EP3R participants.

A.5 Timescale

The above approach will create a small homogeneous motivated task force capable of delivering a high quality proposal in a 6 months timescale.

Annex B: Extract from ENISA Good Practice Guide[7] – Network Security Information Exchanges

What information is shared ?

Information that might usefully be shared in NSIEs would include: incidents, product technical vulnerabilities and risks, protocol vulnerabilities, network intrusion information, probing attacks and network configuration issues within standards.

To maintain trust NSIEs 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.

The following descriptions of what is shared have been observed:

1. Experience - Sharing experience on threats, attacks, counter measures, response, cooperation, etc;
2. Advice - Advisory support in implementing protective measures;
3. Alerts - Alert service on attacks and incidents;
4. Analysis - Information on cyber security, analysis on threats, risks, impact and vulnerabilities, incidents, security measures, etc;
5. Contingency planning - Information on contingency planning, analysis on threats, risks, impact and vulnerabilities, on single point of failures, dependencies, crisis management arrangements, incidents, exercises, etc;
6. Warnings - Everything from security advisories to warnings and best practices;
7. Other - Any type of information which is deemed interesting and valuable in order to support increasing the NSIE members information security, is collected, disseminated and shared;
8. Peer good practice;
9. Incidents and vulnerabilities and also discussions around good practices and recent trends and developments;
10. Physical and Personnel - Information, physical and personnel security information is collected from a wide range of sources.

[7] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu