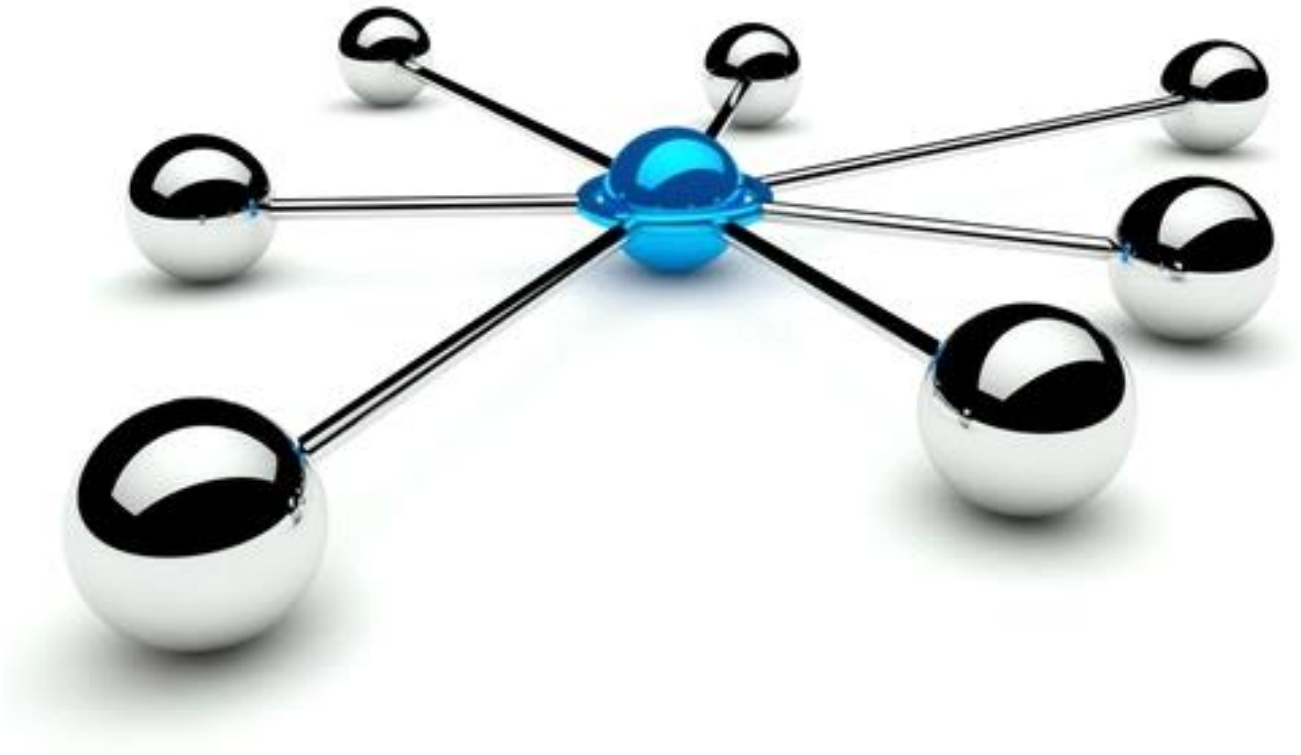
enisa
European Network and Information Security Agency



EISAS

Enhanced Roadmap 2012

[Deliverable – November 2012]

About ENISA

The European Network and Information Security Agency (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

Follow us on Facebook Twitter LinkedIn Youtube & RSS feeds

Contact details

To contact ENISA for this report please use the following details:

- Email: opsec@enisa.europa.eu
- Internet: www.enisa.europa.eu

Contents

List of Figures

1 EISAS Rationale and background

Cyber security is generally in the hands of specialists who implement technical solutions. Citizens and SMEs (Small and Medium Enterprises) are left out of this action despite the fact that a thorough awareness of end users about cyber security is the first line of defence against cyber threats. As such, these players must be provided with the skills to protect their devices, their data and their online identity. No firewall or security policy can efficiently protect users if they are not sufficiently aware of the risks they are facing. As European Commissioner Nelly Kroes has said, "Cyber security is also about ensuring ordinary computer users are 'Web Wise'"[1].

To continually raise the level of cyber security awareness of all citizens and businesses, the European Commission decided to promote a **collaborative approach** for awareness raising in Europe. Introduced in 2006[2], EISAS, the **E**uropean **I**nformation **S**haring and **A**lert **S**ystem, aims to enhance the cooperation of Member States in their work to reach out to citizens and SMEs with relevant security information. In this way, Member States can contribute not only to their own safety and security, but also to a more resilient public communication infrastructure.

In view of its role in fostering a culture of Network and Information Security in Europe, ENISA was requested to "examine the feasibility of a multilingual European Information Sharing and Alert System (EISAS)", in which EISAS would build upon and link together existing or planned national public and private initiatives. The EISAS feasibility study[3] was published in 2007.

The importance of functioning information- and alert-sharing systems that target citizens and SMEs was further emphasized in 2009 by the European Commission in its Communication on Critical Information Infrastructure Protection - COM (2009)149[4]:

"The Commission supports the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects. ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS".

EISAS is further addressed in the EU Internal Security Strategy in Action[5]. One of the five objectives aims to raise levels of security for citizens and businesses in cyberspace:

---

[1] *Opening speech of the European Cyber-Security Month*

[2] *Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" {SEC(2006) 656}*

[3] *"EISAS, A Feasibility Study", 2006-2007, https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf*

[4] *See COM(2009) 149 on CIIP - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience": http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:DOC*

"Firstly, every Member State, and the EU institutions themselves should have, by 2012, a well-functioning CERT. (…). Secondly, Member States should network together their National/Governmental CERTs by 2012 to enhance Europe's preparedness. This activity will also be instrumental in developing, with the support of the Commission and ENISA, a European Information Sharing and Alert System (EISAS) to the wider public by 2013 (…)".

[5] *See COM(2010) 673 final, "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF*

2 Previous work

The feasibility of EISAS has been continually analysed and investigated. Three documents describe the analyses and investigations to date:

- EISAS, A Feasibility Study[6]
- EISAS Basic Toolset, Feasibility Study of Home Users' IT Security[7] and the Enhance report[8]
- EISAS Large-Scale Pilot[9]

2.1 EISAS Feasibility Study

ENISA's study investigated the basic requirements for the possibility of the EISAS becoming a reality. The main findings include the following elements:

- Member States have varying capabilities to sustainably reach their citizens and SMEs with Network and Information Security (NIS)-related information. In the majority (74%) of cases, national/governmental CERTs (n/g CERTs) are involved.
- Solution should be based on national capabilities.
- The role of ENISA should be that of a facilitator, a clearinghouse for good practice information and a knowledge and contact broker.
- Member states should entrust their n/g CERTs to play key roles in the deployment of EISAS. The possibilities to develop and deploy EISAS within a public-private partnership (PPP) must be explored.

2.2 EISAS Basic Toolset

In 2011, ENISA furthered the EISAS approach by developing dissemination methods, and tested this approach in a pilot project on awareness-raising information aimed at citizens and SMEs within one Member State.

This experiment introduced a three-step methodology for EISAS, as shown in Figure 1.

Figure 1: EISAS Basic Toolset three-step methodology

---

[6] *"EISAS, A Feasibility Study", 2006-2007, https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf*

[7] *"EISAS Basic Toolset, Feasibility Study of Home Users' IT Security", ENISA, http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-basic-toolset*

[8] *"EISAS (enhanced) report on implementation", ENISA, http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-report-on-implementation-enhanced*

[9] *"EISAS Large-Scale Pilot, Collaborative Awareness Raising for EU Citizens & SMEs", ENISA, http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder*

This study found the following key success factors in enhancing the reach and outreach of IT security education measures for home users:

- Address employees in their roles as home users directly by email or other means of personal contact by a trusted person or entity of the organisation.
- Provide information and tools tailored to the target groups. A "one-size-fits-all" approach will not work.
- Provide mechanisms that take alerts and helpful information immediately to users in need of them.

The approach and experiment formed a Basic Toolset that defined the basis to a larger experimental deployment involving several Member States: the EISAS Large-Scale Pilot, run in 2012.

2.3 EISAS Large-Scale Pilot

The EISAS Large-Scale Pilot tested the feasibility of the collaborative approach proposed by the European Commission across various Member States. The project refined the three-step methodology defined in the EISAS Basic Toolset (Figure 2) and introduced three roles in the process (Figure 3):

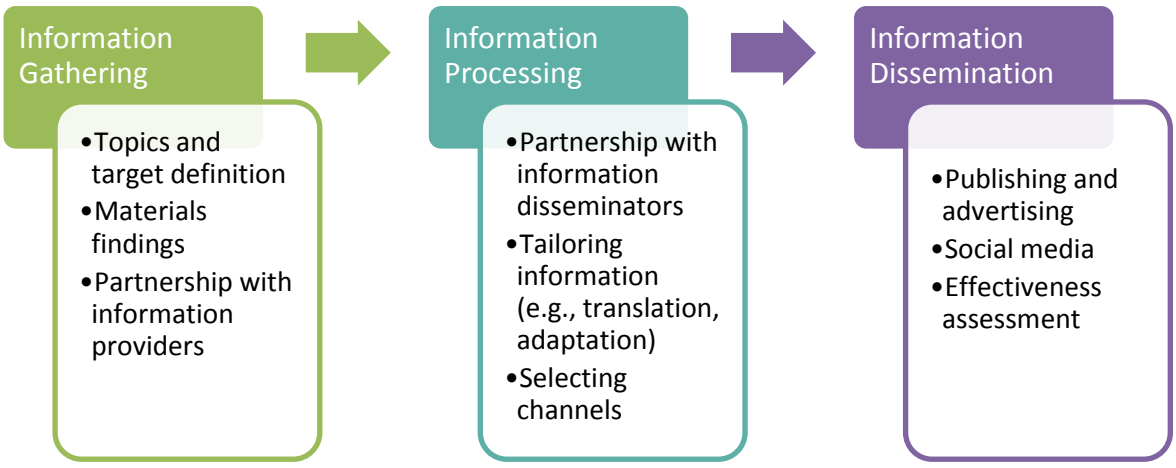


Figure 2: Activities involved in the EISAS processes

1. **Information provider**
   A stakeholder in the information security area who can provide information that is suitable for dissemination beyond its original context. The information provider is expected to distribute information and to help disseminators get information security material to their target groups.
2. **Information disseminator**
   An information disseminator is an entity such as a CERT or other n/g body involved in awareness raising that is willing to disseminate new information. The information disseminator knows the needs of the target audience and is able to distribute

information security. The information disseminators can directly publish information through their own channels or may rely on other local communities.

3. **Information broker**
   The information broker connects information providers and information disseminators and does the necessary coordination work to enable effective collaboration. The role of the broker is to ensure cooperation among the main actors and to assist, when needed, in the processing of information to be disseminated.

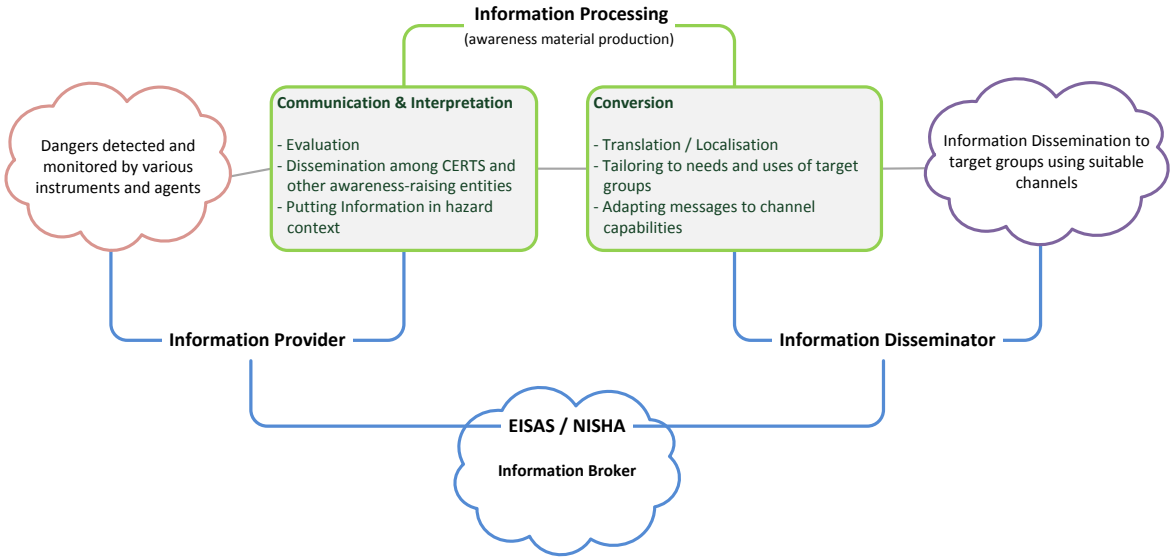


Figure 3: Actor roles and information flows in the EISAS model

The most important outcome of the pilot is that the EISAS approach of a European collaboration in awareness raising works and offers an efficient solution to better the preparedness of EU citizens facing ever-evolving cyber threats.

However, the pilot also showed that such collaboration must be fostered by a brokering actor. Therefore, EISAS needs an entity acting as an information broker and facilitator for its actors that helps with the following functions:

- providing advice for original information producers on how to produce internationally distributable materials;
- building up an incentive system that makes it worthwhile for original information producers to become information providers (e.g., fostering PPPs);
- bringing information providing and information disseminating partners together in teams;
- providing services that help in producing professional translation and localisation of materials and in overcoming technical obstacles;
- instituting collection best practices over time, thus possibly making the information brokering entity unnecessary in the end.

3 Next steps

The three studies referred to above conclude that EISAS can be implemented in the EU. Information providers – private and public – are willing to provide high-quality awareness material for dissemination by n/g CERTs and other entities concerned with awareness raising. Information disseminators who want to use this material are willing to expend time and effort in doing the dissemination.

However, as the outcomes of the recent Pilot project show, EISAS needs **a brokering entity** to operate EISAS and **a technical infrastructure** to ease the transport of information between information providers and information disseminators.

3.1 Assessing a brokering entity

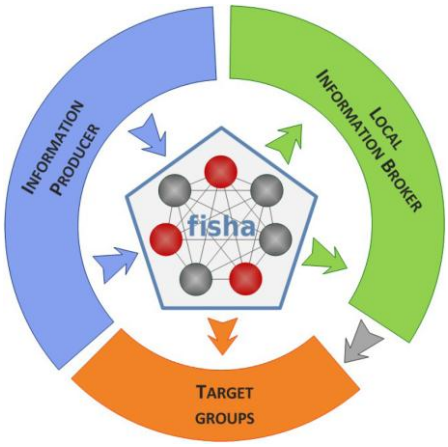
The EISAS pilot confirms that a situation in which dissemination and consumption of IT security information runs without some form of supervision or monitoring is highly improbable, at least in the early phases of community building. The tasks of the information broker are too comprehensive and voluminous to be taken over by information providers and information disseminators in a self-organising way and at their own expense.

This observation calls for a brokering entity to establish links between the actors. In that matter, PPPs should be encouraged. The information broker could itself be a PPP with the task of gathering and processing information that is then ready for dissemination by n/g CERTs in the Member States.

3.2 EISAS technical infrastructure

The brokering entity cannot effectively exchange all information among participants by itself, however. In addition, EISAS needs a technical infrastructure to transport security information among the stakeholders.

To that end, two EU-funded prototyping projects – FISHA[10] and NEISAS[11] – were finalised in 2011. The FISHA project has initiated a network of IT security teams that have agreed to put into a standard format the relevant security information that they usually process to inform and alert end users.



As a follow-up of FISHA, NISHA is now being developed to full functionality until the first quarter of 2014. NISHA is designed as a peer-to-peer network at the European level operated by core nodes (actors) and used by local nodes.

[10] *FISHA – Framework for Information Sharing and Alerting, http://old.fisha-project.eu/*

[11] *NEISAS – National and European Information Sharing and Alerting System, http://www.neisas.eu/*

This infrastructure is a promising candidate to support the information brokerage role required by EISAS.

3.3 ENISA's supporting actions for 2013

ENISA will continue to support the build-up of EISAS. The specifications of EISAS are now well defined and field proven. However, the way in which the system will be deployed in practice still needs to be determined. As stated in its work program for 2013, ENISA will run a **deployment study** which will provide guidelines on how to effectively deploy the EISAS in the EU. This activity will take stock of the results from the previous pilot project but also from the EU-funded NISHA project by assessing the effectiveness of this infrastructure. The feasibility study will also explore the possible collaborations and partnerships to support the essential brokerage activities of EISAS.

In summary, the EISAS enhanced roadmap involves the activities indicated in Table 1.

Activity	Timeline
Development of NISHA	2012-2013
ENISA's deployment study: Information Brokering and Sharing infrastructure for EISAS	End of 2013
Further possible steps *(to be confirmed by the deployment study)*	
Deployment of NISHA	
Setting up of the EISAS brokering entity	
EISAS running	

Table 1: EISAS activities and timelines

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu