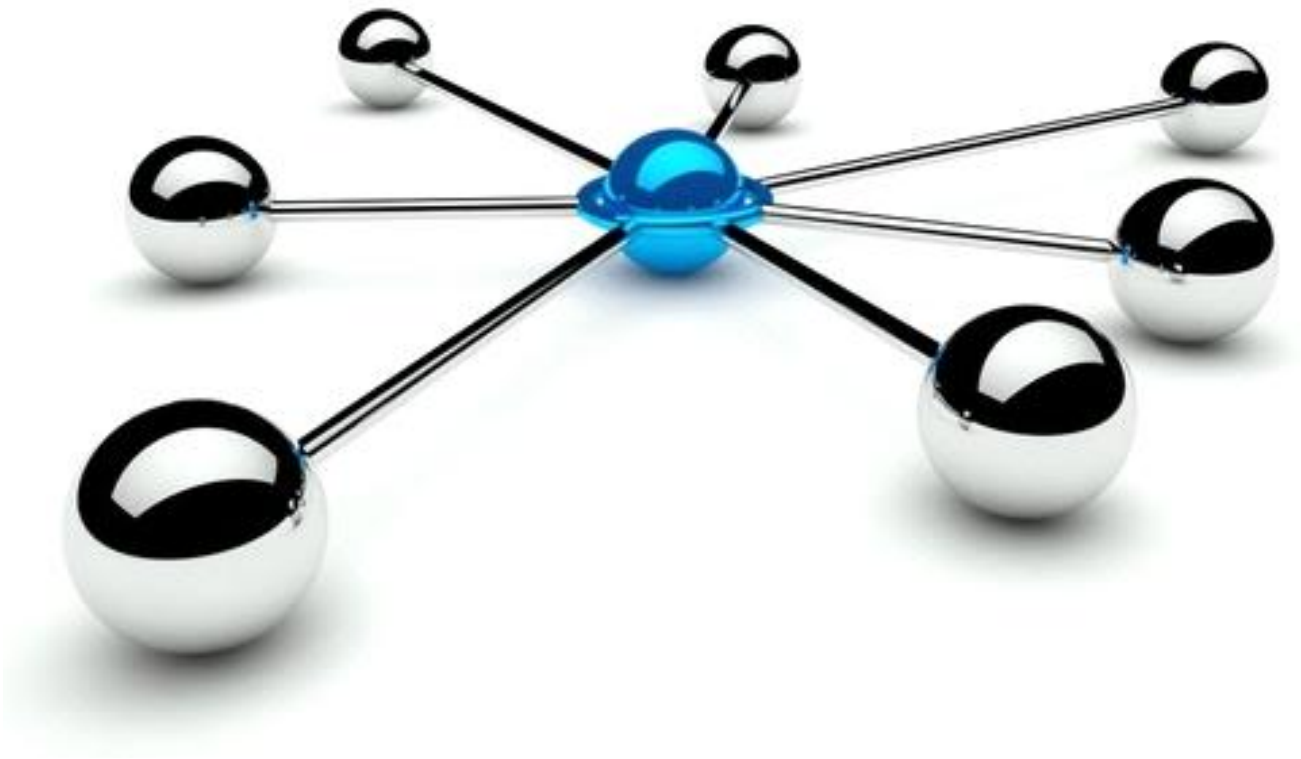
enisa
European Network and Information Security Agency



EISAS Large-Scale Pilot

Collaborative Awareness Raising for EU Citizens & SMEs

[Deliverable – November 2012]

Contributors to this Report

This EISAS Pilot project was commissioned by ENISA to the Ludwig-Maximilians-Universität München in Munich, Germany (LMU Munich, http://www.lmu.de/).

Author of the report: Dr Werner Degenhardt, LMU Munich

Project manager and report editor: Romain Bourgue, Expert in Network and Information Security, ENISA

Agreements and Acknowledgements

We would like to express our deep appreciation to all the contributors the EISAS Pilot who actively contributed to this project. Our special thanks go to Bence Birkás (CERT Hungary), Katarzyna Gorzelak (CERT Polska), Ivan Monforte Fugarolas (CESICAT) and Raúl Amigorena Eguíluz (La CAIXA).

We also wish to express our sincere and highest gratitude to the information providers Deutsche Telekom AG and NorSIS. Their generous contributions of high quality materials for awareness raising were necessary to the success of this project. In this regards, we specially thank the personal support of Josef Paulik (DTAG) and Tore Orderløkken (NorSIS).

Acknowledgement should also be given to ENISA colleagues who contributed to this project, in particular: Cosmin Ciobanu, Lauri Palkmets, Jo De Muynck and Andrea Dufkova.

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

1 Executive summary 1
2 Introduction 3
2.1 Citizen and SME awareness landscape in Europe 3
2.2 Rationale and background 4
3 EISAS Pilot methodology 8
3.1 Large-scale and collaborative approach 8
3.2 Applying the EISAS model 10
3.2.1 Information gathering 10
3.2.2 Information processing 11
3.2.3 Information dissemination 11
3.3 EISAS Pilot stakeholders 12
3.3.1 Information provider 13
3.3.2 Information broker 13
3.3.3 Information disseminator 13
4 Pilot preparation 14
4.1 Finding motivated stakeholders 14
4.2 Stakeholder tasks 14
4.3 Awareness-raising materials used 15
4.3.1 Text/pictures 15
4.3.2 Flash quiz 16
4.3.3 Interactive video 16
4.4 Participating stakeholders 17
4.4.1 Deutsche Telekom AG 17
4.4.2 NorSIS 18
4.4.3 CESICAT 18
4.4.4 CERT Polska 19
4.4.5 Biztonsagosinternet hotline (CERT Hungary) 20
4.4.6 La Caixa 21
5 Pilot execution 22

5.1 Stakeholder communication 22
5.2 Material preparation 22
5.2.1 Availability 22
5.2.2 Rights considerations 22
5.2.3 Translation 23
5.2.4 Programming and technical infrastructure 24
5.2.5 Tailoring 25
5.3 Material dissemination 27
5.3.1 CESICAT Catalunya 27
5.3.2 Biztonsagosinternet hotline (CERT Hungary) 28
5.3.3 CERT Polska 29
5.3.4 La Caixa 30
5.3.5 Summary 31
5.4 Project management 31
5.5 Time and effort 32
6 Dissemination outcomes 34
6.1 Citizens 34
6.2 SMEs 38
6.3 Participants 39
7 Conclusions and recommendations 40
7.1 Main findings 40
7.2 Lessons learned 40
7.2.1 Project management 40
7.2.2 Programming 41
7.2.3 Dissemination 41
7.2.4 Human factors 41
7.2.5 Information broker 42
7.3 Next steps 43
7.3.1 NISHA, the promising sharing infrastructure 43
7.3.2 Fostering Cooperation 43

8 Annex I: References 45

9 Annex II: Abbreviations 47

10 Annex III: EISAS Pilot Participants 49

List of Figures

Figure 1: EISAS Basic Toolset three-step methodology 7
Figure 2: EISAS Large-Scale Pilot blueprint 9
Figure 3: Activities involved in the EISAS main processes 10
Figure 4: Actors and information flows in the EISAS model 12
Figure 5: A Botmaster with its bots 15
Figure 6: NorSIS ID Theft test 16
Figure 7: Bluff City – Social Engineering Video 16
Figure 8: Bluff City – Interactive Part 17
Figure 9: DTAG mySecurity Base 17
Figure 10: EISAS Pilot hosting infrastructure 26
Figure 11: SE material Spanish version for la Caixa 30
Figure 12: La Caixa Security Bulletin announcing the SE movie 31
Figure 13: Clickstream graphic – from announcement to viewing the awareness material 37

List of Tables

Table 1: CESICAT Catalonia links to disseminated materials 28
Table 2: Biztonsagosinternet - Links to disseminated materials 29
Table 3: CERT Polska – Links to disseminated materials 30
Table 4: EISAS Pilot - EU wide collaboration characteristics.....32
Table 5: Time and effort in person-days expended by participants in the EISAS Large-Scale Pilot 33
Table 6: Awareness material views from 29 August to 13 October 2012 34
Table 7: Reach of EISAS announcement among the 507 CERT.PL followers on Facebook 35
Table 8: Referrals to EISAS Pilot awareness material presentation on CESICAT website 36
Table 9: Participants.....49
Table 10: Information brokers 49

1 Executive summary

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].

A recent Eurobarometer survey[2] reveals that most EU citizens feel unprepared to protect their online information. Also unfortunate, most efforts to raise their awareness are targeting limited audiences: employees of a company or, at best, specific groups of citizens of a country.

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[3], 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.

This year, following the *EISAS Roadmap*[4] recommendation published in 2010 and the *EISAS report on implementation*[5] published in 2011, ENISA ran the *EISAS Pilot* project. This project follows the recently successfully tested three-step methodology that is defined in the *EISAS Basic Toolset*[6]: Information Gathering, Information Processing and Information Dissemination.

Within the framework of the *EISAS Pilot project*, national/governmental CERTs (Computer Emergency Response Teams) and other communities in Germany, Hungary, Portugal, Norway, Spain and Poland that agreed to participate gathered into a collaborative and cross-border awareness raising effort. Innovative awareness raising materials were obtained from major actors at a national level. An international team was set up to collaboratively process and adapt the materials to the needs and particularities of every stakeholder's population. These

---

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

[2] *Special Eurobarometer 390, "Cyber Security Report", http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf*

[3] *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}*

[4] *"EISAS Roadmap, A Roadmap for further development and deployment", ENISA, http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap*

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

[6] *"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*

materials were then disseminated by using appropriate communication channels (social media, large public websites, specialised mailing lists, among others) targeting EU citizens and SMEs.

In due course, this large-scale pilot reached more than 1500 people. Citizens and SMEs across Europe were empowered with security knowledge to protect themselves against some of today's most critical cyber threats: Botnets, identity (ID) theft and social engineering.

However, the achievement of this pilot project goes beyond raising citizens' awareness; it also shows that the EISAS approach of a **European collaboration in awareness raising works and offers a cost-effective solution** to better prepare EU citizens facing ever-evolving cyber threats.

The results achieved from this pilot have now to be built upon through continued collaboration, and this pilot showed that such **collaboration needs to be fostered by a brokering actor**. Therefore, EISAS needs an entity to act as information broker and facilitator. ENISA had taken this role in this project, but it now has to be transferred to a collaborative community of willing stakeholders. In this regard, the infrastructure being constructed this year by the NISHA project –Network for Information Sharing and Alerting (NISHA), project complementary to EISAS and co-funded by the Directorate General for Home Affairs (DG HOME)[7] – is a promising candidate to support the information brokerage required by EISAS.

[7] *For more information on the NISHA project, see http://nisha-network.eu/*

2 Introduction

2.1 Citizen and SME awareness landscape in Europe

A recent Eurobarometer survey[8] requested by the European Commission shows that Internet users are very concerned about cyber security: 89% avoid disclosing personal information online and 74% agree that the risk of becoming a victim of cybercrime has increased in the past year. Of the Internet users across the EU, 12% have already experienced online fraud and 8% have fallen victim to identity theft. Nonetheless, 53% have not changed any of their online passwords during the past year, and most EU citizens (59%) do not feel well informed about the risks of cybercrime.

"While ever more people are making the most out of the Internet and benefit from the digital economy, it is not surprising that security of personal information and online payments top the list of our concerns. What is more surprising is that only half of Europeans take effective measures to protect themselves from cybercrime", said Cecilia Malmström, EU Commissioner for Home Affairs[9].

The survey, covering a total of almost 27,000 people in all EU Member States, shows a strong link between being informed about the risks of cybercrime and feeling confident online. More than half (59%) of those who feel confident in their ability to do online banking or buying goods online say they feel well informed about cybercrime.

"Cybercriminals must not be allowed to disrupt our use of the Internet. The more we know about the risks and how to protect ourselves, the more we can truly maximise our digital lives", warns Malmström.

---

[8] *Special Eurobarometer 390, "Cyber Security Report", http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf*

[9] *http://ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_en.htm*

2.2 Rationale and background

A call for pan-European awareness raising actions

In everyday life, citizens at work or at home are dependent on using computers and mobile phones as part of the digital economy and information society. However, increased connectivity also brings increased cyber threats. Therefore, this greater dependency on digital economy also calls for greater security in this online world. Given this importance for society and its citizens and the exposure to emerging cyber threats, it is critical that organisations across Europe turn users and SMEs into a first line of defence by raising their security awareness: awareness raising is essential for empowering citizens with the knowledge and behaviour needed to fight cyber threats.

Regrettably, most of the European entities involved in awareness raising have a limited constituency, and therefore their activities are restricted to a small community, to a company or, at best, to the citizens of a single Member State. Cyber threats, however, do not stop at national borders; they are not confined to one country, a specific enterprise or a careless home user. All citizens and enterprises are involved and targeted. These risks on a globally interconnected system call for global readiness, and therefore require **global and coordinated security awareness actions**.

Furthermore, citizens and SMEs across Europe are not equally prepared to protect their information. As reflected in recent studies[10], the *digital divide* among EU citizens not only shows a discrepancy in information accessibility but also reflects a digital divide in information security. In other words, digitally less developed Member States are not only suffering in terms of access to the Internet but they are also prone to deficits in information security when accessing the Internet. The capabilities of national/governmental CERTs (n/g CERTS) and other agencies responsible for the security of the IT infrastructure or involved in awareness raising are not on par across EU Member States[11].

To highlight the importance of global awareness-raising actions, the European Commission has identified the key role for Member States in keeping home users and SMEs properly informed so that they can contribute to their own safety and security. Subsequently, in 2006, the Commission introduced, in its communication *A Strategy for a Secure Information Society*, the notion of "a **E**uropean **I**nformation **S**haring and **A**lert **S**ystem, EISAS […] in order to improve the European capability to respond to network security threats"[12].

---

[10] *See, for example, Van Deursen & Van Dijk (2010) and Van Dijk (2005) for background information on this subject.Fighting digital ignorance is one of the top priorities of the European Commission (Guarascio 2011).*

[11] *See the recent status report on "Deployment of Baseline Capabilities of National/Governmental CERTs", ENISA (2012).*

[12] *http://ec.europa.eu/information_society/doc/com2006251.pdf*

EISAS Feasibility Study

In this communication, the European Commission asked ENISA to *assess the feasibility* of EISAS. The resulting Feasibility Study was published in 2007.[13] It analyses the current state of affairs with regard to existing systems and initiatives in the public and the private sectors in the EU Member States, and identifies possible sources of security information that could potentially contribute to a Europe-wide information-sharing and alert system.

The main findings of ENISA's study on EISAS feasibility 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, n/g CERTs are involved. The predominance of CERTs in this area results from the expertise that these teams have in collecting, processing and sharing information to conduct their core services of incident response and alerting/warning. Both long-term good IT security practices, and short- to mid-term security advice on recent and upcoming threats are provided to citizens and SMEs.
- A centralised solution that directly shares information at a European level with citizens and SMEs is less likely to be accepted than a solution based on national capabilities. Existing mechanisms and activities must be taken into account and, more important, should contribute to EISAS. 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. A successful and accepted deployment of EISAS can be achieved only by efficient cooperation among Member States in general and their n/g CERTs in particular. The possibilities to develop and deploy EISAS within a public-private partnership (PPP) must be explored.

The study concludes that the most effective level of involvement for the European Union in the establishment and operation of an information-sharing system for its home users and SMEs would be that of a facilitator, moderator of discussion and a “keeper of good practice”.

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

The EISAS Roadmap

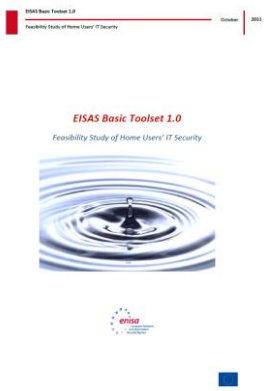
The importance of functioning information- and alert-sharing systems targeting citizens and SMEs was further emphasized in 2009 by the European Commission in its Communication on Critical Information Infrastructure Protection - COM (2009)149[14]:

"*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*".

This communication also called upon ENISA to *produce a roadmap to further the development and deployment of EISAS.*

The EISAS Roadmap, published by ENISA in February 2011, introduced a step-by-step approach to develop EISAS with the final objective to fully deploy EISAS by 2013[15].

The EISAS Basic Toolset



According to the EISAS Roadmap, the basic functionalities and services of EISAS were to be developed and integrated in a regional prototype in 2011: the EISAS *Basic Toolset*[16]. This prototype was to be extended to larger communities in 2012 in the EISAS Large-scale Pilot project.

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

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

---

[14] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "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:PDF*

[15] *EISAS Roadmap, "A Roadmap for further development and deployment", ENISA; https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap*

[16] *"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*

Figure 1: EISAS Basic Toolset three-step methodology

This straightforward methodology was tested on a subset of German citizens and SMEs and was proven successful by using a *test-intervention-retest* approach. A target population of citizens and employees was pre-tested on their security knowledge. Then, an awareness-raising campaign involving disseminated material on how to protect against Botnets targeted this specific population via an information website and an employee mailing list. The effectiveness of the dissemination was evaluated with a post-dissemination test that assessed the increase in the population's security knowledge, change of security attitudes and actual security behaviour.

This approach and experiment formed a Basic Toolset that defined the basis to a larger experimental deployment involving several Member States; this is the EISAS Large-Scale Pilot, running in 2012 and detailed in this report.

The EISAS enhanced report on implementation

Following the Basic Toolset experience, ENISA gathered European experts from n/g CERTs and other entities involved in awareness raising to comment on and define the future of EISAS. The expert group actively supported the idea of an EISAS Large-Scale Pilot in 2012 and insisted on the importance of cross-border cooperation to tackle information-sharing issues. The experts also presented at least partial funding from the governments as a precondition for realising EISAS[17].

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

3 EISAS Pilot methodology

3.1 Large-scale and collaborative approach

In 2011, the European Commission released a communication on Critical Information Infrastructure Protection (COM 2011 – 163)[18], which established concrete actions targeting the most urgent security challenges that Europe is facing. One key action of this plan is to enhance EU readiness by founding *a network of well-functioning n/g CERTs* by 2012. In this communication, a collaborative network of n/g CERTs is expected to be *the backbone of EISAS for citizens and SMEs* by *establishing a network of contact points between relevant bodies and Member States*.

Ultimately, EISAS has three combined goals:

- **to empower all EU citizens and SMEs** with the knowledge and skills necessary to protect their IT systems and information assets,
- **to build on national capabilities** of EU Member States, and
- **to enhance cooperation** between n/g CERTs and other entities involved in awareness raising.

Therefore, EISAS will, once it is fully deployed, support the Member States in delivering relevant security information to citizens and SMEs, thus representing an important component in the EU's Critical Information Infrastructure Protection (CIIP) policy. In addition, it is intended that EISAS will be the product of the benefits gained from effective collaboration among EU Member States, particularly n/g CERTs, as well as other entities that are involved in raising awareness. Consequently, the goal of a deployed EISAS should be seen as equally important as the means to reach that goal.

ENISA introduced, in its 2012 Work Program under the work stream *Supporting the CERT and Other Operational Communities,* the task of the *development and deployment of EISAS*. Following the identified goals of EISAS, the aim of this task was to facilitate a pilot for EISAS deployment in one Member State. This large-scale deployment pilot will focus on two main aspects: **collaboration among the relevant key players**, and **sharing and distributing good-practice information**. A blueprint of this project is shown in Figure 2.

[18] *Com2011-163 on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security"; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF*

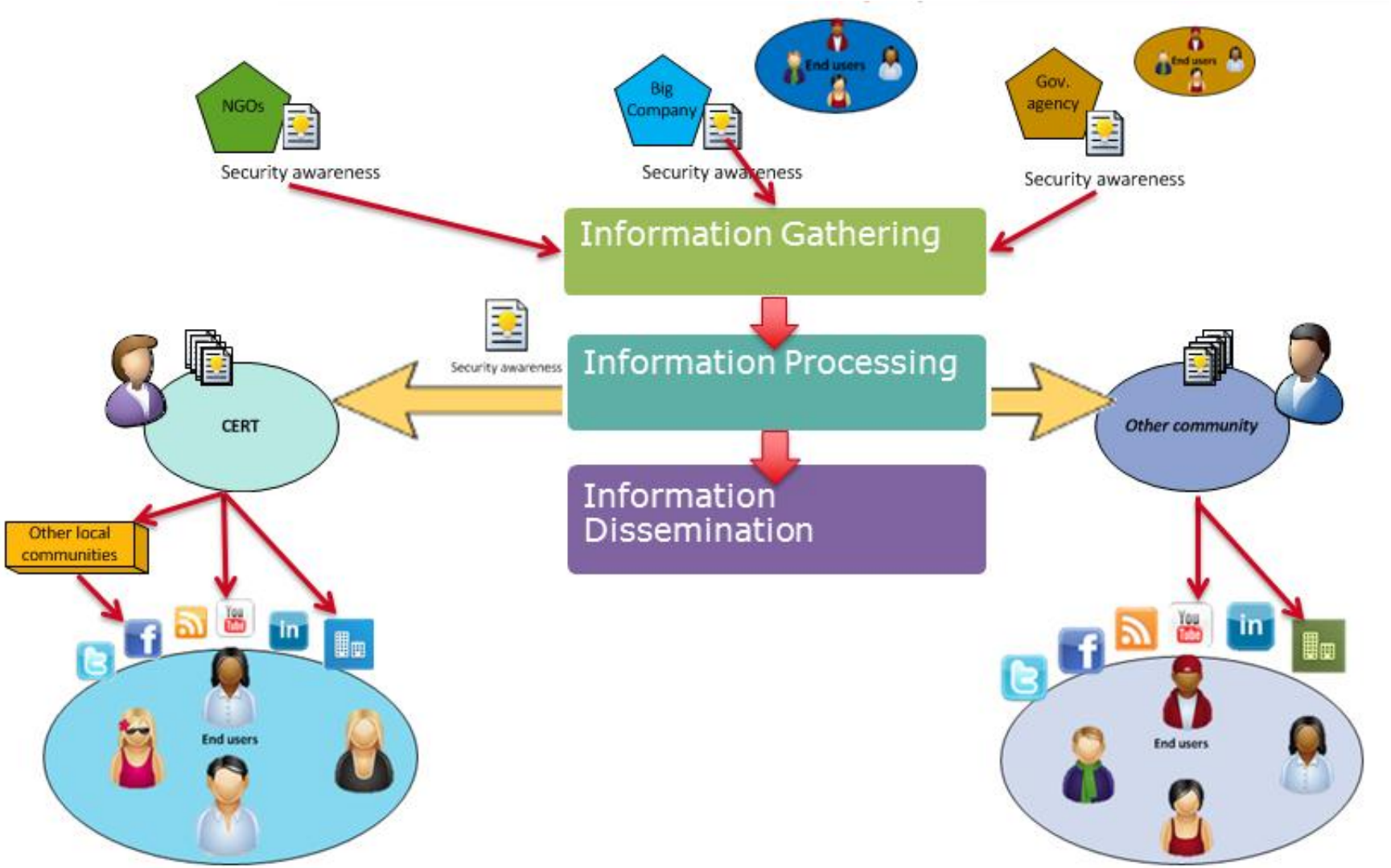


Figure 2: EISAS Large-Scale Pilot blueprint

3.2 Applying the EISAS model

The three-step methodology introduced in the EISAS Basic Toolset was further enhanced by drawing upon the body of research on hazard warning systems, which elaborates many aspects of EISAS.[19] Figure 3 presents the activities involved in these three steps, which are elaborated in the remainder of this section.

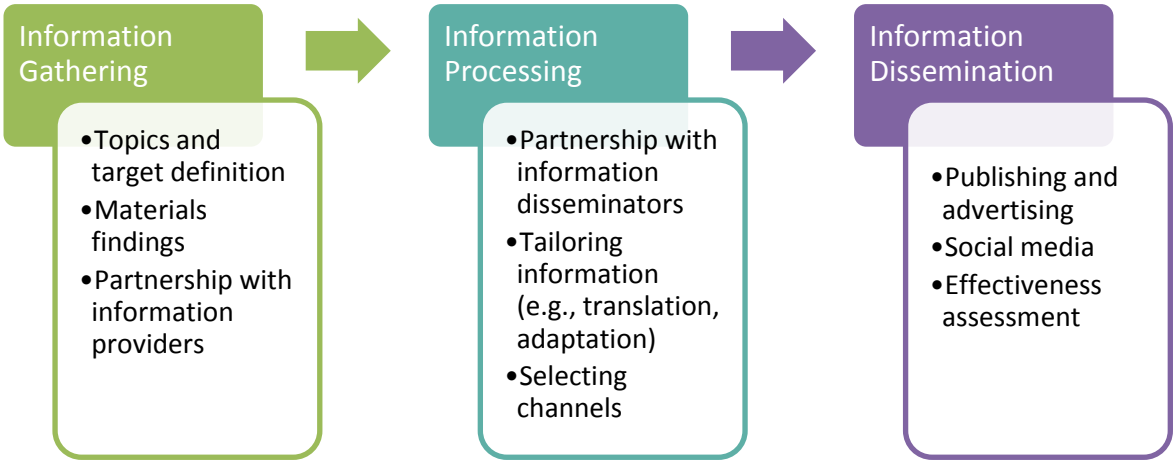


Figure 3: Activities involved in the EISAS main processes

3.2.1 Information gathering

In the model introduced by EISAS, *information gathering* represents the *hazard detection and monitoring* part of every alert system. In the case of EISAS, the hazard detection and monitoring task is tackled by CERTs and other agencies involved in raising awareness.

As in any awareness-raising campaign, this first step involves identifying topics to be addressed and defining the target groups. This is a key element, as most successful awareness-raising actions recognize that the message and the target should be in accordance with each other.

Once the awareness-raising objectives are defined in terms of topics and target, the EISAS Pilot coordinators can gather existing awareness-raising materials from among the possible stakeholders to address the identified topic or threat. This implies establishing a partnership with possible information providers. The EISAS approach involves building on national capabilities; this means partnerships with existing local actors addressing citizens and SMEs. The best source of awareness-raising material includes non-governmental organisations

[19] *The paper by Samarajiva (2005) contains much good advice for building a distributed hazard warning system in a multinational environment.*

(NGOs), large public or private companies and established national/governmental entities involved in awareness raising.

3.2.2 Information processing

In the international approach of EISAS, the gathered information selected for dissemination has to be tailored to fit the specific target populations. Tailoring involves not only translating, but also an elaborated process that includes adaptation of content to the needs and uses of the various nationalities, cultures and target groups. Different audiences represent different viewpoints and require different messages. The need to define the specific audience targeted by an awareness initiative is decisive for tailoring the message content with respect to not only language but also the knowledge or technical aptitude of the recipients by using the most effective communication channels. Those channels may also have their own characteristics to be taken into account when tailoring awareness-raising materials to be disseminated.

In contrast to a "*one size fits all"* approach, personalised tailoring of information maximises the appeal of the message and persuades the audience to take action, especially if the message fits with the target group's interests and needs.[20]

Therefore, there is a need for closer collaboration with information disseminators. They are the ones who know their target population best as well as the characteristics of the dissemination channels that will be used.

3.2.3 Information dissemination

Raising awareness is about communication with people. This step follows a communication plan defining the digital places, the dates, the channels and the actions used to disseminate the awareness-raising materials. Once the awareness-raising materials are tailored to the dissemination channels and targets, it is time to implement the specific communication plan.

Awareness raising is often an ongoing process within a continual improvement approach. Therefore, assessing the effectiveness of a dissemination campaign is equally essential. Measuring the ability to improve information security and change people's behaviours can be difficult. To this end, the EISAS Pilot takes into account the findings of the *EISAS Basic Toolset,* which proved that a tailored message reaching a population in need of information effectively improves its global information knowledge.

Currently, social media represent a great opportunity not only to actively promote information and reach a population in demand of information, but also to measure the impact of the information dissemination. The EISAS Pilot takes advantage of the special media dissemination vectors to reach the target groups, advertises the dissemination and provides measures of its effectiveness.

---

[20] *See ENISA (2010), "The New Users' Guide: How to Raise Information Security Awareness".*

3.3 EISAS Pilot stakeholders

A stakeholder involved in EISAS can be any party that has an interest in the success and ongoing operation of an information technology infrastructure within the EU. The individual stakeholders, even though they share a common interest in the health and security of the IT Infrastructure, can and will have slightly different perspectives.

In the case of EISAS, the types of stakeholders, as shown in Figure 4, are

- information providers,
- information brokers,
- information disseminators and
- information consumers.[21]

Any stakeholder can play any role in the EISAS model over time.

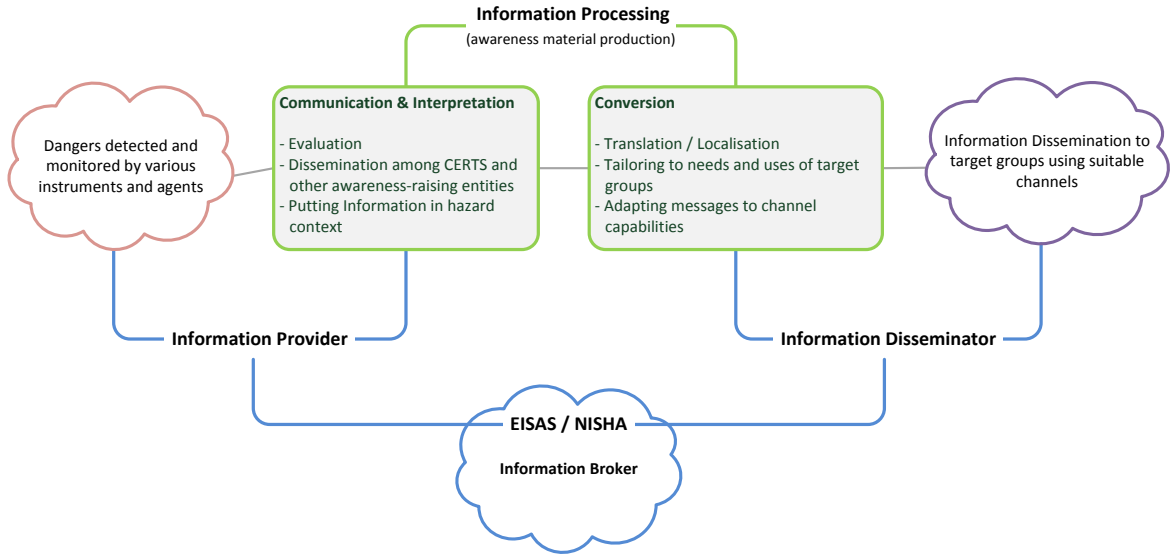


Figure 4: Actors and information flows in the EISAS model

EISAS acts on the assumption that there are two main roles in gathering/processing and disseminating information security materials:

[21] *Citizens and SMEs are often omitted from the list of stakeholders because they are considered passive and less organised than the entities that represent providers, brokers and disseminators. However, citizens do act upon the material presented. In the worst case, they ignore the information and help provided to them, but in any case they interpret what they learn according to their own situational and personal contexts. See, for example, Dourish et al. (2004) for a good description of how everyday users, outside the confines of an organisational IT department, deal with IT security.*

1. **Information provider:** A stakeholder in the information security area who can provide information that is suitable for dissemination beyond its original context.

2. **Information disseminator**: A stakeholder willing to disseminate information security materials available from information providers; these usually are not in a condition appropriate for use by the intended information receiver.

Additionally, an **information broker** is needed to bring the two roles into contact.

3.3.1 Information provider

The information provider is expected to distribute material to help disseminators get information security material to their target groups. Suitable information comes in the form of ready-to-use materials, and thus legal, technical and collaborative aspects have to be handled before the process can start.

3.3.2 Information broker

The information broker connects providers and 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.

As part of its facilitator responsibility in the EISAS Pilot project, ENISA took over the role of information broker.

3.3.3 Information disseminator

An information disseminator is an entity such as a CERT or other national or governmental entity 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 materials to those audiences, provided the material is properly converted for the needs, uses, skills and understanding of those audiences.

The information disseminators can directly publish information through their own channels or they may rely on other local communities if they offer better dissemination channels. To that end, local SMEs, WARP[22] communities and national/governmental entities involved in awareness raising can also be stakeholders of the information dissemination process.

[22] *Warning, Advice and Reporting Points; http://www.cpni.gov.uk/*

4 Pilot preparation

4.1 Finding motivated stakeholders

The most important resource needed to run EISAS is a set of motivated stakeholders who are willing to provide and disseminate IT security-related information and materials.

The ability to provide and disseminate awareness materials involves several essential prerequisites:

- Usable awareness materials must be available.
- The content of the awareness materials has to be adaptable in terms of language as well as political and cultural characteristics of the various target groups.
- The technical demands of the material should not require heavy reprogramming or special and expensive infrastructure.
- The costs related to copyrights of disseminated materials should be acceptable.

Finding stakeholders that are both able to provide suitable awareness materials punctually and are willing to contribute sufficient time and energy to go through the necessary tasks for their dissemination is a very challenging undertaking that should not be underestimated. Finding motivated stakeholders is a task assigned to the information broker.

4.2 Pilot actors tasks

As shown in Section 3.4, stakeholder tasks comprise the following work packages:

1. monitoring the risks of the EU cyber environment in order to identify cyber threats that are most in need of immediate counteraction by awareness raising;
2. producing or gathering awareness materials suited to alter cognition, attitudes and behaviour of citizens and SMEs[23];
3. selecting awareness materials that are suited for distribution and processing in the network of stakeholders in the EU Member States;
4. converting awareness materials to a form suitable for dissemination in the various Member States – this involves the complex process of translation, customisation, tailoring and technical adaptation of the selected awareness materials; and
5. distributing materials to the target groups and monitoring dissemination and awareness-raising success.

As shown by the EISAS Pilot, all of these tasks are collaborative by their very nature and have to be accompanied by a high level of project communication so as to anticipate and solve all those particular problems that usually come along with any large international project.

---

[23] *In fact, there is a long path from raising awareness to changing IT security behaviour (knowledge – attitude – skills – intentions – behavior); see ENISA (2011b), page 8 ff. Standard psychological knowledge posits that it is difficult to change behaviour by changing knowledge and attitudes; see Fishbein (1975) and Ajzen et al. (1980).*

4.3 Awareness-raising materials used

The German Federal Office for Information Security (BSI) runs a register of cyber threats.[24] According to this register, the top six attack vectors are:

1. targeted hacking of web servers in order to place malware or to prepare espionage of connected networks and databases;
2. drive-by exploits to infiltrate end users' computers with malware to make those computers members of a Botnet;
3. targeted malware infiltration via phishing or other social engineering techniques to gain control of a computer;
4. distributed denial of service attacks with the goal of disrupting the Internet connectivity of the services of an organisation;
5. non-targeted distribution of malware via spam or drive-by exploits leading to identity theft;
6. staged attacks that first compromise central security infrastructures and then go for the real targets.

On the basis of this list of attack vectors, the participants decided that, for this pilot, awareness-raising material to be disseminated to citizens and SMEs should address:

- safe surfing and Botnets,
- phishing and social engineering, and
- identity theft.

Another consideration in locating and selecting awareness materials was the nature of the material, as this influences its attractiveness for the target population. The following content formats were chosen:

- text/pictures,
- flash quiz, and
- interactive flash video.

4.3.1 Text/pictures

A web guide for fighting Botnet infections and keeping the home personal computer (PC) clean and healthy was reused from the EISAS Basic Toolset study of 2011 for presenting text.

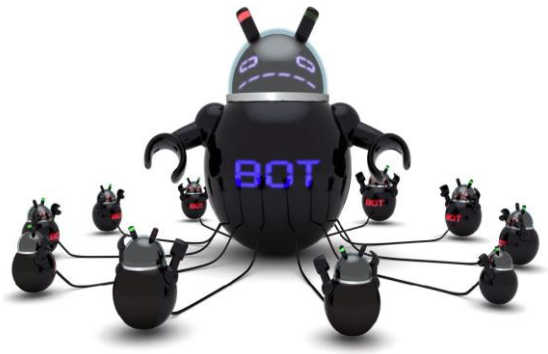


Figure 5: A Botmaster with its bots

[24] *https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Analysen/Grundlagen/BSIa001.html*

This web guide is a textual explanation on how Botnets and Trojans work, why this is dangerous for the home user and how a user can stay safe. The web guide contains links to a video explaining the nature of malware and links to tools that do health checks of PCs.

4.3.2 Flash quiz

The flash quiz is a self-assessment test and informational training on being secure against ID theft and fraud involving people's IDs. With this approach, the users can evaluate their own level of readiness and can learn how to better protect their identity. The test is part of a larger project initiated by NorSIS to fight fraud on the Internet.[25]

Figure 6: NorSIS ID Theft test

NorSIS (Norsk senter for informasjonssikring/Norwegian Centre for Information Security) is the Norwegian governmental entity whose aim is to raise the security awareness of Norwegian citizens. The source code of the ID Theft test (see Figure 6) was released under the Creative Common licence, and NorSIS provided it to the EISAS Pilot project. This made it possible to adapt the ID Theft test to the languages spoken in the Member States of the information disseminating participants.

4.3.3 Interactive video

The most advanced material obtained for use in the EISAS Pilot is an interactive video produced for use in a large awareness campaign of Deutsche Telekom AG (DTAG) to alert its employees to the dangers of social engineering. This social engineering campaign is part of a sequence of campaigns to strengthen the human firewall in the company and its branches as well as subsidiary companies. The Bluff City movie was technically prepared to be rolled out worldwide in many languages and is thus ideally suited for use in this EU-wide project.

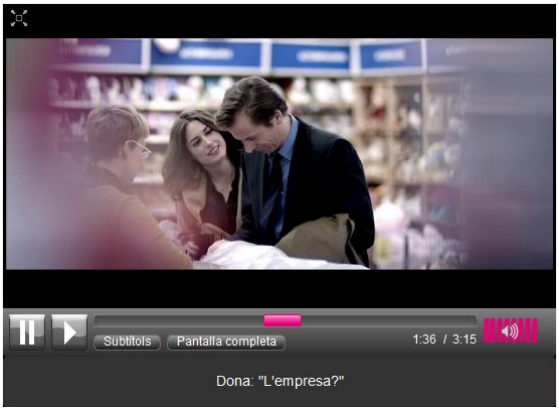


Figure 7: Bluff City – Social Engineering Video

The interactive video is a two-part flash application. The first part (Figure 7) is a short movie of an employee falling into social

[25] *http://www.idtyveri.info/index.php?option=com_content&view=article&id=119:about-the-id-theft-project&catid=38:engelsk&Itemid=30*

engineering traps. The story ends badly: the main character's professional information is stolen, ruining a very important project. In the second part of the video (Figure 8), an interactive game allows the player to turn the tide of the story by choosing the correct behaviour to protect against social engineering and, in the end, have a happy ending.

Figure 8: Bluff City – Interactive Part

4.4 Participating stakeholders

The EISAS Pilot had six participants. Information providers were

- DTAG ,
- NorSIS.

Participants taking the role of information disseminators were

- CESICAT,
- CERT Hungary (Biztonsagosinternet hotline),
- CERT Polska,
- la Caixa.

4.4.1 Deutsche Telekom AG

Deutsche Telekom AG (DTAG) proved to be the most important information provider participating in the EISAS Pilot[26]. Their awareness material was of high quality in content and technology, and their project team was motivated and invested in time as well as money in procuring everything necessary to get commercially produced material ready for public use. This is not an easy task and normally takes longer than the six-month time frame available for conducting the EISAS Pilot.

Internally, the Social Engineering movie used in this project – and, in fact, many more materials of interest for awareness information disseminators in the EU – were presented on a web application called mySecurity Base (Figure 9), which is designed for use in the DTAG international

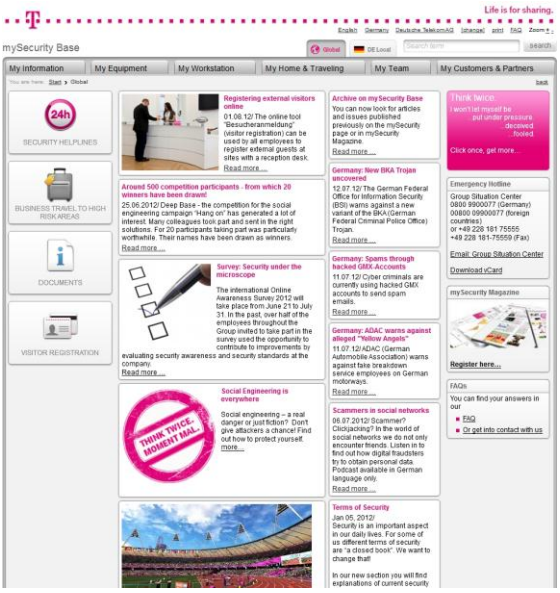


Figure 9: DTAG mySecurity Base

[26] http://www.telekom.com/home

environment.

High-quality material requires a significant budget not easily found in organisations that usually produce publicly available material. Therefore, governmental organisations and NGOs concerned with IT security usually do not have as many resources available for IT security awareness and training as do larger EU private companies.

Since those large companies also have information security policies not only in the company but also for the environment of a company, there should be natural opportunities for a public/private partnership in information security between EISAS and the companies of Europe.

4.4.2 NorSIS

NorSIS is the Norwegian Centre for Information Security and is part of the Norwegian government's overall commitment to information security. NorSIS works towards information security being considered a natural part of everyday life through:

- raising awareness about threats and vulnerabilities;
- advising on specific measures through news and guidance; and
- influencing positive attitudes in information security.

NorSIS TV

NorSIS is not a CERT but is a governmental entity actively involved in awareness raising. It has a strong orientation towards citizens and SMEs, and it follows an interesting approach to awareness raising with NorSIS TV[27] on its website.

4.4.3 CESICAT

CESICAT is the agency responsible for promoting information and communications technologies (ICT) security. The agency was approved by the government of the Generalitat of Catalonia on 17 March 2009.

The mission of the Catalonia National Plan is to ensure a secure information society for everyone in Catalonia and to operate CESICAT.

The National Plan for the promotion of ICT security in Catalonia is structured around four main strategic objectives:

[27] *http://www.norsis.no/tv/*

- Execute the national strategy for ICT security established by the government of the Generalitat of Catalonia.
- Support the protection of a national critical ICT infrastructure.
- Promote a reliable ICT security system for the Catalan business community.
- Increase confidence and protection of Catalan citizens in the information society.

Within these strategic objectives, CESICAT was created as an auxiliary and instrumental entity of the government of the Generalitat of Catalonia. CESICAT also acts as the CERT for Catalan SME, citizens, universities and public administration. As such, CESICAT CERT is a member of FIRST[28] and accredited by Trusted Introducer[29].

4.4.4 CERT Polska

The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) – a research institute that conducts scientific activity, operates the national domain registry (.pl) and provides advanced IT network services.

CERT Polska is the first Polish computer emergency response team. Active since 1996 in the environment of response teams, it became a recognised and experienced entity in the field of computer security. Since its launch, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. It also conducts extensive research and development into security topics.

In 1997, CERT Polska became a member of FIRST, and since 2000 it has been a member of the working group of European response teams – TERENA TF-CSIRT[30] and an associated organisation Trusted Introducer. In 2005, on the initiative of CERT Polska, Abuse FORUM, a forum of Polish abuse teams, was created. In 2010, CERT Polska joined the Anti-Phishing Working Group[31], an association of companies and institutions that actively fights online crime.

The main tasks of CERT Polska include:

- registration and handling of network security incidents for Poland and the .pl domain name space;
- providing watch and warning services to Internet users in Poland;
- offering active response in cases of direct threats to users ;
- cooperation with other CERT teams in Poland and worldwide;
- participation in national and international projects related to IT security;

[28] *Forum of Incident Response and Security Teams; http://www.first.org/*

[29] *http://www.trusted-introducer.org/*

[30] *http://www.terena.org/activities/tf-csirt/*

[31] *http://www.antiphishing.org/*

- research activity in relation to methods of detecting security incidents, analysing malware, and providing systems for exchanging information on threats;
- developing proprietary tools for detection, monitoring, analysis, and correlation of threats;
- regular publication of the CERT Polska Report on the security of Polish online resources;
- providing information and education activities aimed at increasing awareness in relation to IT security, including publishing security information at www.cert.pl and Facebook and Twitter social networks organising the annual SECURE conference; and
- performing independent analyses and testing solutions related to IT security.

4.4.5 Biztonsagosinternet hotline (CERT Hungary)

Biztonsagosinternet ("Safe Internet" in Magyar) is a service by the Theodore Puskas Foundation that also runs CERT Hungary[32]. The Theodore Puskas Foundation has been providing an online reporting service since May 2011 to tackle illegal and harmful content hosted on the Internet. Its hotline was established as a part of the Safer Internet Plus project as a partner of the Hungarian Safer Internet consortium. The project is supported by the European Commission.

The hotline handles the following categories of illegal and harmful content (partial list):

- child sexual abuse images (pictures, videos);
- cyberbullying;
- harmful, violent content;
- racial hatred content;
- enticement to drug consumption; and
- content published without the owner's approval.

The main goal of the hotline is to take down unlawful content as soon as possible. Harmful content can be defined as any kind of website or online video, picture, and text that can be detrimental to the growth of the young generation. The main objective of the Theodore Puskas Foundation is to minimise these threats and take down illegal and harmful contents or restrict them from children. To achieve these goals, they are working together with the Hungarian police, Internet service providers, and members of INHOPE, the International Association of Internet Hotlines.

[32] *http://www.cert-hungary.hu/en*

4.4.6 La Caixa

The Caja de Ahorros y Pensiones de Barcelona, "la Caixa", is the result of a 1990 merger between the Caja de Pensiones, founded in 1904, and the Caja de Barcelona, founded in 1844.[33] From its beginnings, la Caixa was primarily dedicated to offering family savings and private pensions to all its customers when this type of welfare service did not yet exist in Spain. Thus, since its origins, la Caixa has been characterised by a strong social commitment and a vocation to work in the general public interest, both through its financial activity and its welfare projects, which finance activities of a social, cultural and scientific nature.

[33] *http://lacaixa.es/*

5 Pilot execution

5.1 Stakeholder communication

A pre-existing relationship of trust among key actors in information providers' and information disseminators' organisations was vital for the success of the EISAS Pilot project. The author of this report was involved in the social engineering awareness campaign of Deutsche Telekom, which initiated the Social Engineering (SE) movie. One subcontractor had a long-standing relationship to NorSIS, which contributed the ID Theft quiz. Most of the information disseminators are involved in NISHA, a project complementary to EISAS (see Section 7.3.1).

Nevertheless, a planning workshop had to be arranged with both Deutsche Telekom and NorSIS to define the project environment for the key actors and agree on acceptable risks and workloads.

Also, there were personal relations from the information brokers ENISA and Ludwig-Maximilians-Universität München (LMU) to the information-disseminating participants. This is not to say that without pre-existing trust among the collaborators an EISAS would be impossible, but the time and effort needed to build a relationship of trust from scratch would not have been possible within the time frame of this pilot.

5.2 Material preparation

5.2.1 Availability

Awareness material suited for EISAS must be available before it can be used. This sounds straightforward, but in reality it proved to be complex due to the issue of availability.

Availability implies the following.

- **The material is allowed to be used freely within the EU**, with no restrictions on target groups, countries, languages, or other factors, and all copyright and other legal considerations are well-regulated.
- The material can be **localised with acceptable effort**; that is, content characteristics, cultural peculiarities and language can be adapted to the requirements of the individual target groups.
- The **programming requirements** for making a localised version of the available material does not entail complete redesign.
- The **technical infrastructure** required to disseminate the material does not overstrain the capabilities of the disseminating partner.

5.2.2 Rights considerations

According to the participants, the most valuable awareness material used in the EISAS Pilot was the Social Engineering movie provided by Deutsche Telekom AG. The SE movie is a commercially produced piece of art and was originally licenced for internal use within the

confines of the organisation and its branches. To be able to use the movie in the EISAS Pilot, Deutsche Telekom had to provide a public license.

It can well be imagined that the processes to arrive at such a decision are far from being easy and fast. High-quality material comes with a price tag and can rarely be given away without taking copyright and licence fees into consideration. An animated movie explaining Botnets[34] was also considered for use within this project. It turned out, however, that the effort required to handle yet more copyrighted material would have overburdened the project.

5.2.3 Translation

Translation of awareness-raising materials suitable for dissemination does not involve just the translation of a piece of text from one language to another.

Botnet web guide

Even the translation of the least technically demanding material – the Botnet text – presented the problem that it contained links to video material on the Internet and to software for inspecting the security state of the computer. Links to video material are a natural way to enhance textual presentations on the Internet, but – at least in the technical realm – this requires switching from a translated text to an English-language video in many cases. What goes almost unnoticed for security specialists can be an insurmountable obstacle for citizens and SMEs. And, in the Botnet example, there was just no video on Botnets available in the national language of the information disseminators and also no localised version of the PC inspection software.

ID Theft flash quiz

The ID Theft test confronted the information brokers at LMU with the problem that the original test used a font and character set that prevented the representation of characters of the Polish and Magyar alphabet.

Changing the character set and font also changed the on-screen appearance and proportions of the ID Theft test. To aggravate things further, words and sentences translated from one language to another result in changed text length, so that graphics had to be reworked.

It took some experimentation and an experienced flash programmer to arrive at a satisfactory solution.

---

[34] *On YouTube, http://www.youtube.com/watch?v=XlSc8W5VaR8; on the BSI BuergerCERT Website, https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html; on the GovCERT NL website, http://www.govcert.nl/onderwerpen/Animatiefilm+over+virussen+en+wormen*

Bluff City – Social Engineering interactive movie

When localising the SE movie, it became apparent that there are many approaches to getting film material adaptable to other languages and cultures. Interestingly, the SE movie deals with security information[35] in an easier way than an animated film, which was also considered for use in this project. The voice-over animation approach of the animated film required the voice to be remixed to fit the film for any language in question, and that is a costly endeavour in terms of time and money.

The SE movie included few words but was rich in everyday emotionally loaded situations. As a use test[36] showed, subtitling the German language version in Hungarian was not acceptable. The speaker's voice and – interestingly – the animations distracted from reading and understanding the subtitles. The same approach (German language speakers, Hungarian subtitles), however, did not pose a problem in the SE movie. In the end, a global approach of an English audio version and localized subtitles proved to be the most suitable format for every disseminating participant.

The conclusion is that decisions regarding rendering awareness-raising video material adaptable and attractive should be made in the early design phase of the production of the material. For the SE movie, the action movie approach proved to be superior in many ways to the instruction film approach used in the Botnet video.

Translation was done by professional translators with experience in information technology texts (Polish, Magyar) or by the information disseminators themselves (Catalán, Spanish).

5.2.4 Programming and technical infrastructure

Content shown in the Internet needs a technical infrastructure and code that processes the content on this infrastructure. Any combination of complexity is possible. The information broker unit at LMU was able to take a glimpse into what could be required during the adaption of material to the hosting requirements of a peered multinational environment.

Not all materials are equally adaptable

The localisation of the SE movie was straightforward. Subtitles and text were stored in two xml files. The xml file content was then translated, connected to the flash file of the video, and linked to a calling website.

The localisation of the ID Theft quiz involved basically the same procedure with the notable difference that the translated text had to be manually put into the flash program. Differences in programming style within the ID Theft quiz, use of graphical representation of characters, and a character set that did not include foreign characters made adaptation time consuming.

---

[35] *http://www.govcert.nl/onderwerpen/Animatiefilm+over+virussen+en+wormen*

[36] *The information broker unit at LMU did many tests in the course of getting the materials online by using a "bargain-basement" usability testing approach; see Krug (2005) and Nielsen (1999).*

The infrastructure required is an obstacle for seamless dissemination

Whereas the hosting of text material is straightforward, the hosting of flash videos and the incorporation of the flash videos into the disseminators' websites proved to be more demanding. Getting a flash video to behave properly according to the design requirements of a hosting website and the peculiarities of the hosting CMS is not easy.

In the end, the result was a rather widespread peered web hosting arrangement due to the constraints on the participants of the EISAS Pilot and the results of trials (Figure 10). In the end, the technical components of the pilot were distributed over the sites of all information brokers and information disseminators.

The disseminating participants were not able to host the flash material for a variety of technical and policy reasons. Therefore, all flash applications were hosted on a special server at LMU. LMU also hosted the text parts of the materials on another server for CERT Polska. CERT Polska could not host the awareness material, but did advertise it in the social channels (Facebook, Twitter). The EISAS participants in Catalonia and Hungary integrated the awareness materials into their websites and linked to LMU only for the flash applications ID Theft test and SE movie.

The lesson to be learned is that it is neither straightforward nor easy to integrate technically complex material in existing websites. If we follow the advice of IT security research and move from presenting awareness-raising material to applying embedded training to users when they fall prey to cyber threats[37], we will certainly have to tackle the problem of how to design and implement advanced interactive e-learning environments in a collaborative hosting environment.

5.2.5 Tailoring

Tailoring is required to make awareness material fully integrated into what a disseminating participant in EISAS thinks fits best to the offerings for the various target groups being served.

CESICAT of Catalunya went to great lengths to integrate the material into the look and feel of the CESICAT website; CERT Polska and la Caixa, in contrast, relied on other means to make the materials known to their target groups, such as Facebook, Twitter and email bulletins.

All in all, the conclusion is that awareness material is not readily available for international dissemination even if the first impression tells otherwise. Considerable time and energy has to be expended to make existing material available for dissemination by others, to solve rights issues, to translate, and to tailor the materials to channel and target group characteristics.

[37] *Jakobsson (2007); Kitten (2012)*

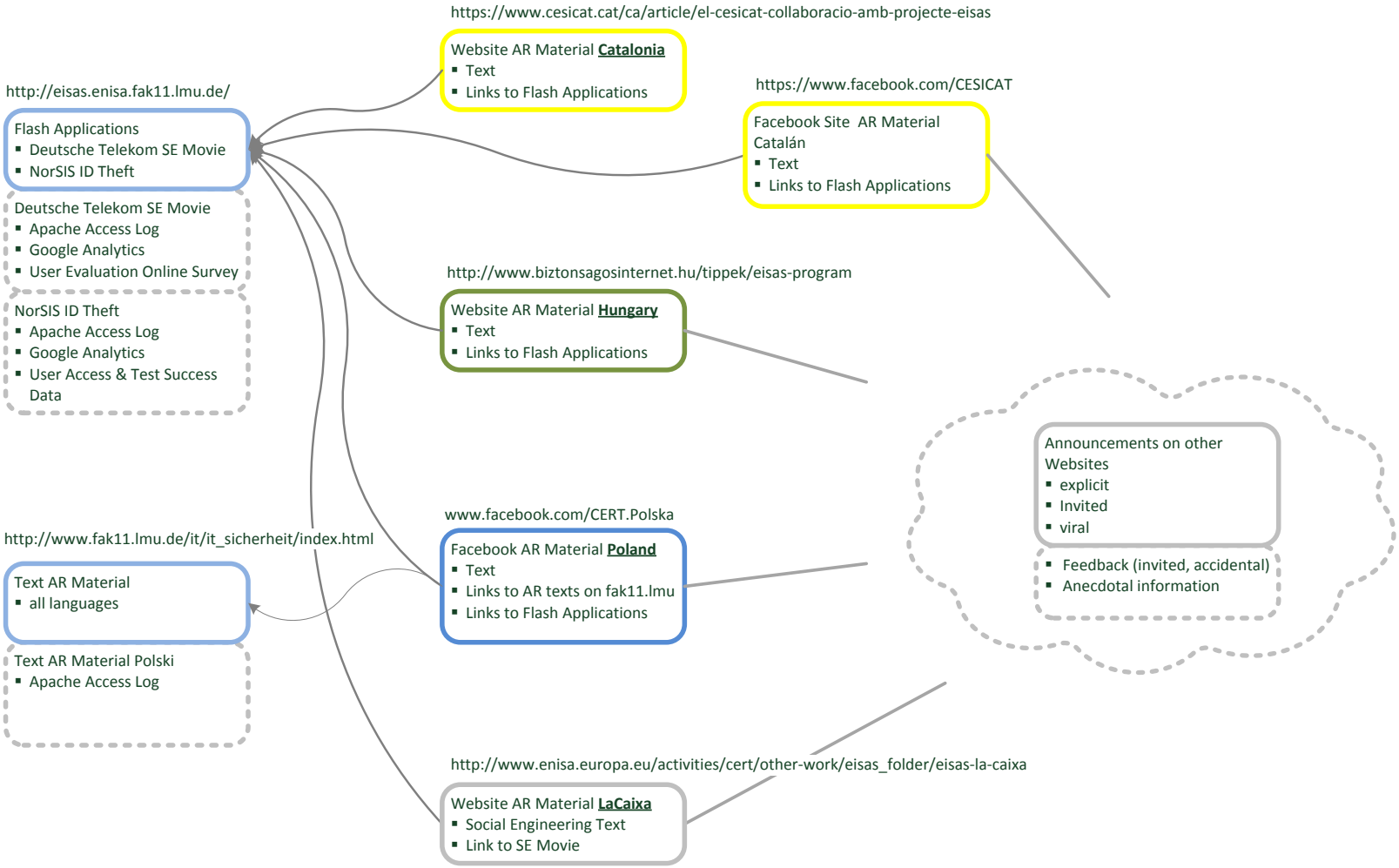


Figure 10: EISAS Pilot hosting infrastructure

5.3 Material dissemination

5.3.1 CESICAT Catalunya

CESICAT disseminated all three materials on its website and also a Facebook site (see Table 1). Following this dissemination, CESICAT actively tweeted to alert followers to the new material.

"*Què és el robatori d'identitat?*" and the Botnet materials were first shown on the CESICAT site on 21 August 2012, and the video "*La Enginyeria Social*" was disseminated on 23 August 2012.

On 24 August 2012, CESICAT published an introductory "*El CESICAT en collaboració amb el projecte EISAS*" text on the collaboration between ENISA and CESICAT and, in fact, the appearance of the site was as if it was an EISAS site.

CESICAT went to great lengths to fully integrate the material into the website. Format, content and information were considered so attractive and interesting that CESICAT ran a full-blown advertising campaign. To attract people's attention, they sent Twitter messages from the CESICAT profile. They twitted a different message daily in an effort to promote the didactic material about everyone's security.

At the end of this campaign, CESICAT had sent 11 Facebook messages and 43 tweets.

cesiCAT – Links to the disseminated materials		
Officials sites	CESICAT website	https://www.cesicat.cat/ca/article/el-cesicat-collaboracio-amb-projecte-eisas
	CESICAT Facebook	https://www.facebook.com/CESICAT
	CESICAT Twitter	https://twitter.com/cesicat
Botnet Material	Com funciona un botnet?	https://www.cesicat.cat/ca/article/com-funciona-botnet
ID Theft	Què és el robatori d'identitat?	https://www.cesicat.cat/ca/article/que-es-el-robatori-identitat
	ID Theft test	http://eisas.enisa.edu.lmu.de/idtheft/catalan/
Deutsche Telekom – Social engineering	Vídeo: La Enginyeria Social	https://www.cesicat.cat/ca/article/video-enginyeria-social
	Survey to the video	https://survey.fak11.lmu.de/mrIWeb/mrIWeb.dll?I.Project=SEMOVIEcat
	Què és la Enginyeria Social?	https://www.cesicat.cat/ca/article/que-es-enginyeria-social

Table 1: CESICAT Catalonia links to disseminated materials

5.3.2 Biztonsagosinternet hotline (CERT Hungary)

The Biztonsagosinternet hotline disseminated all three materials in the course of the EISAS Pilot (see Table 2).

The materials were disseminated on the main website of the Biztonsagosinternet hotline, and other web-based channels, such as the Facebook page of Biztonsagosinternet, were used to spread the information provided by the EISAS Pilot.

The materials were made public on 29 August 2012, and are still available on the Biztonsagosinternet hotline.

Announcements on several websites informed people about the start of the program, all providing a direct link to the original Hungarian content. There was no special advertisement or public relations campaign to announce the publication because there was no budget allocated at CERT Hungary for this purpose.

Some social network activity occurred, however, to foster secondary publication, and all affiliated information disseminators agreed to share the announcement on their websites.

Biztonsagosinternet Hotline – Links to the disseminated materials		
Official sites	Biztonságos Internet	www.biztonsagosinternet.hu
	Facebook	www.facebook.com/biztonsagosinternet/
Botnet material	A botnetekről	www.biztonsagosinternet.hu/tippek/a-botnetekrol
ID Theft	A személyazonosság lopásról	www.biztonsagosinternet.hu/tippek/a-szemelyazonossag-lopasrol
	ID Theft test	eisas.enisa.edu.lmu.de/idtheft/magyar/
Deutsche Telekom – social engineering	A social engineering-ről	www.biztonsagosinternet.hu/tippek/a-social-engineering-rol
	Interactive Video	eisas.enisa.fak11.uni-muenchen.de/Telekom/Bluffhu.html
	Survey to the video	survey.fak11.lmu.de/mrIWeb/mrIWeb.dll?I.Project=SEMOVIEHU
Press and related coverage	EISAS – program az európai állampolgárok biztonságáért	http://www.orientpress.hu/104315/RSS
	Biztonságosabb netet!	http://www.hirextra.hu/2012/09/17/biztonsagosabb-netet/
	A Biztonságosinternet Hotline részt vesz az EISAS programban	http://tech.cert-hungary.hu/tech-blog/120827/a-biztonsagosinternet-hotline-reszt-vesz-az-eisas-programban

Table 2: Biztonsagosinternet - Links to disseminated materials

5.3.3 CERT Polska

CERT Polska published all three materials on their social sites. CERT Polska uses social networks as the most effective Internet medium for disseminating information. They announced the materials in two stages in order to reach a higher amount of recipients. First, on 3 September 2012, they announced each material individually, and then, three weeks later, as a complete set. The first approach on Facebook took place on 3 September 2012, and on 26 September 2012, announcements took place on Facebook, Twitter, and a blog. See Table 3 for CERT Polska links to disseminated materials.

The materials triggered interest among information brokers who follow CERT Polska on its social channels, and they disseminated it further.

CERT Polska considers itself a rather technically oriented team. The material it usually posts on the social channels is mostly relevant to technical recipients. Thus, the established dissemination channels are not intensely followed by producers of non-technical content and awareness brokers. CERT Polska has tried to communicate with potentially interested portals oriented, for example, at seniors (senior.pl), but had no response prior to the conclusion of the EISAS Pilot.

CERT Polska – Links to disseminated materials		
Official sites	CERT Polska	www.cert.pl
	Facebook	www.facebook.com/CERT.Polska
	Twitter	twitter.com/CERT_Polska
Blog entry	Czy jesteś podatny na kradzież tożsamości? Sprawdź się!	www.cert.pl/news/6193
Press and related coverage	Nie dziel się z nikim swoją tożsamością	www.dlp-expert.pl/advice/id,217/nie_dziel_sie_z_nikim_swoja_tozsamoscia.html

Table 3: CERT Polska – Links to disseminated materials

5.3.4 La Caixa

La Caixa selected the SE movie for dissemination. Social engineering is a very important threat for banks because phishing uses social engineering techniques and, in fact, is considered as "computer-based social engineering". The Deutsche Telekom SE movie perfectly depicts a multistage and multiperson social engineering attack and shows how proper security behaviour can prevent harm.

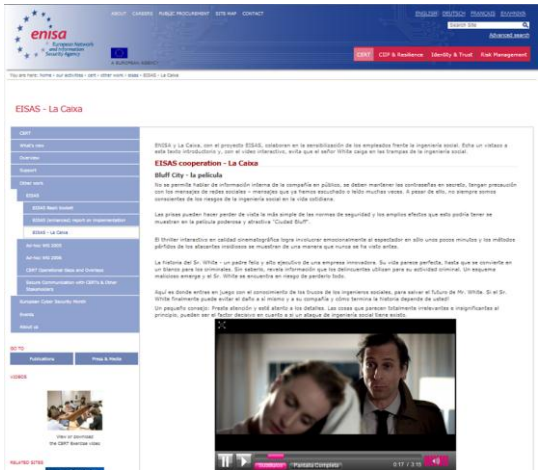


Figure 11: SE material Spanish version for la Caixa

La Caixa chose a *push* strategy to make the material known to its target audience, which consists of about 400 employees in the IT department and other interested persons.

A web page containing an introduction to the SE movie and an explanation of what social engineering is (see Figure 11) was created on the ENISA website.

The link to the presentation of the SE movie was sent out in the Security Bulletin, a bi-weekly email-newsletter part of the security awareness-raising activities published by la Caixa (see Figure 12).

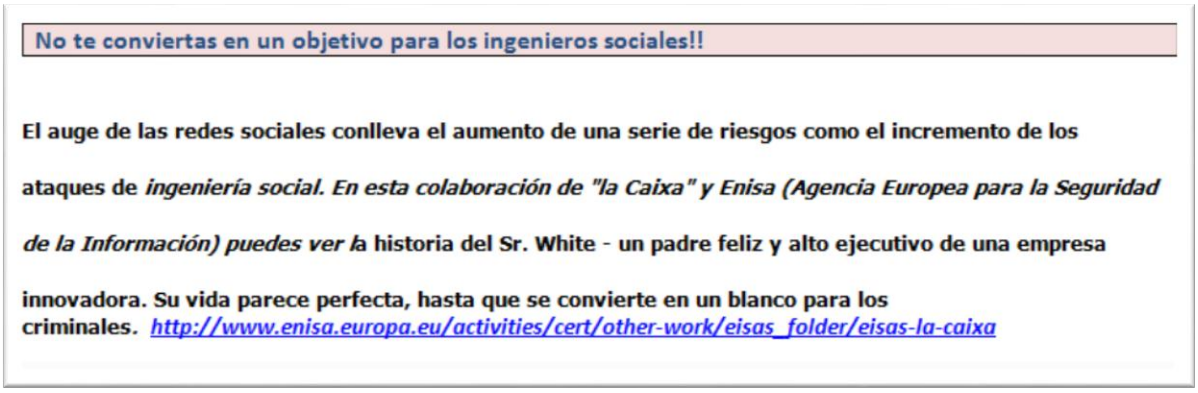


Figure 12: La Caixa Security Bulletin announcing the SE movie

5.3.5 Summary

The dissemination strategies chosen by the participants in the EISAS Pilot covered a wide range of channels and dissemination methods:

- full integration of the material into the hosting website versus providing links to external hosts;
- pull (website only) versus push (mail bulletin, Facebook, Twitter); and
- actively advertising the material versus relying on the attention and interest of visitors to use the material

The effectiveness of the various approaches are described in Chapter 6 (Dissemination outcomes).

5.4 Project management

Obviously, the special conditions of a large international collaborative project based on voluntary work by different participants add significant friction within the project, which has to be handled.

According to Olson[38], friction due to distant collaboration arises from problems with:

- common ground (culture, time zones, local context, language);
- coupling (dependencies) of group work;
- collaboration readiness, the motivation for co-workers to collaborate; and
- collaboration technology readiness, the current level of groupware assimilated by the team.

All of the above conditions applied to the EISAS Pilot (see Table 4). The project involved six countries with their special characteristics and eight languages spoken. The work on highly

[38] *Olson, Gary M., Olson, Judith, S. (2000), "Distance Matters", Human-Computer Interaction, 15 (2-3), 139-178.*

coupled tasks had to cross three time zones and was carried out by 24 persons who had to grasp the idea, accept a responsibility and deliver the collaborative outcome.

Differences	Number	
Countries	6	Denmark (2), Germany (11), Greece (2), Hungary (3), Norway (2), Poland (2), Spain and Catalonia (3)
Languages	8	Catalan, French, Danish, German, Magyar, Norwegian, Polish, Spanish
Time Zones	3	GMT+0, GMT+1, GMT+2
Coupling	Tight	Planning technical setup, solving the 20% left after applying the 80/20 rule[39], tight chaining of tasks (e.g., no programming before finishing the translation, no dissemination before technical setup is error free)
Collaboration Readiness	Medium	Noticeable tendency to treat distance communication like collocated meetings; however high proneness to swift trust[40]
Collaboration Technology Readiness	Medium	Mainly use of classical communication tools such as email with attachments, Skype conferencing; project management Web 2.0 platform was used by two participants only

Table 4: EISAS Pilot - EU wide collaboration characteristics

Many individuals were involved in the project. It can be assumed that altogether about 80 people contributed to make the EISAS Pilot a success.

The project management used a collaboration platform to keep things organised. The fact that everything was online at any time in a well-organised way was an important asset for distant collaboration.

In the end, the number of files produced by the translation of the text components of the materials alone totalled 300 files (source files times languages times versions).

5.5 Time and effort

The fact that collaboration of voluntary actors is able to produce a high-quality IT security awareness campaign at a much lower price than a commercially originated equivalent does

[39] *also called the Pareto principle, http://en.wikipedia.org/wiki/Pareto_principle*

[40] *Jarvenpaa et al. (1998); Jarvenpaa and Leidner (1999). The concept of* swift trust*, which refers to the way that virtual teams can work together fairly quickly once they are able to develop trust among team members, is important because virtual teams are often put together for short-term tasks before being disbanded and re-formed with different team members for another task. The "crisis" element of the work means that there may be little time available to achieve the set objectives.*

not mean that it comes at no cost. In fact, the participants in the EISAS Pilot had to invest considerable time and effort to make the project a success (see Table 5).

All in all, the EISAS Pilot consumed roughly 250 person-days to get to the state described in this report, and 80% of the expenditures were contributed by the information broker. Of the 200 person-days contributed by the information broker, 80% went into project management, programming and documentation.

This is a stunning outcome given the preconception that the distribution of available high-quality awareness material could be somewhat more easygoing and "viral".

Activity	Information Provider		Information Broker	Information Disseminator				
	DTAG	NorSIS	LMU/ENISA	CESICAT	CERT.HU	CERT.PL	La Caixa	**Total**
Availability	3	1	8	-	1	-	-	**13**
Translation	-	-	14	4	3	2	1	**21**
Programming	-	-	46	2	1	1	-	**50**
Tailoring	-	-	4	2	1	-	-	**7**
Dissemination	-	-	15	8	1	1	1	**26**
Project Management	1	1	81	4	2	1	-	**90**
Other	-	-	29	2	1	1	-	**33**
Total	**4**	**2**	**197**	**22**	**10**	**6**	**2**	**243**

Table 5: Time and effort in person-days expended by participants in the EISAS Large-Scale Pilot[41]

[41] *The actual work on the EISAS pilot started in May 2012, and the campaign ran from 29 August to 12 October 2012.*

6 Dissemination outcomes

6.1 Citizens

The materials presented were viewed about 1,600 times during the six-week period from 29 September to 13 October 2012. The materials did not have many returning visitors within the dissemination time frame, so the EISAS Pilot reached roughly 1,500 citizens in the information disseminating countries of Catalonia, Hungary and Poland.

Table 6 shows large differences in the absolute number of views of the awareness materials presented across countries. These variations should not come as a surprise, however. They show that Zipf's law[42] is invariably valid for websites, too: Just put your link on a well-frequented website and you will have many visitors and page views. Since the CERT.PL website is well entrenched and has many views from returning visitors, this naturally spills over to everything that is linked on their homepage.

As the web homepages of CESICAT and Biztonsagosinternet generally receive fewer visitors, all subsites will suffer the same fate. Hence, hits on links with CESICAT and Biztonsagosinternet homepages are expected to poll worse than those with CERT Polska.

Material	Catalonia	Hungary	Poland	Total
SE Movie	120	21	174	**315**
ID Theft	111	12	373	**496**
Botnet	487	11	329	**827**
Total	**718**	**44**	**876**	**1.638**

Table 6: Awareness material views from 29 August to 13 October 2012

CERT.PL relied solely on its Facebook site and Twitter account. CESICAT also invested heavily in its representation on Facebook and Twitter to promote the materials disseminated on its website.

Table 7 summarizes the number of views due to the dissemination on the CERT.PL Facebook site. This shows clearly how views of a Facebook announcement page translate into views of awareness material. Of the N=507 followers CERT.PL has on Facebook, N=291 viewed the announcement of the SE movie and 60% of those views translated into actually viewing the SE movie on the LMU site (N=174, see Table 6).

[42] *Zipf's law describes agglomeration and growth phenomena of all sorts (Zipf 1949).*

In the same manner, N=315 views of the announcement of the ID Theft test translated into N=373 actually taking the test on the LMU site (120%).

It may seem strange that more people took the ID Theft test than viewed the announcement. This can be explained by the effect of tweets on Twitter, word of mouth and other ways one can be connected to information on the Internet.

Material / Reach	Organic	Viral
(1/5) "Jak funkcjonuje botnet", "Jak chronić się przed włączeniem do botnetu?" (Botnet article)	329	6
(2/5) "Czym jest kradzież tożsamości" (About ID Theft)	295	0
(3/5) "TEST: Jak bardzo jesteś podatny na kradzież tożsamości" (ID Theft test)	315	4
(4/5) "Czym jest inżynieria społeczna?" (Description of social engineering)	301	7
(5/5) Social Engineering Awareness Movie	291	3
Czy jesteś podatny na kradzież tożsamości? Sprawdź się! (Link to summary of campaign)	289	3
Note: *The reach definition of Facebook is* ***Organic reach:*** *The number of unique people, fans or non-fans, who saw this post in their news feed, ticker or on your Page.* ***Paid reach:*** *The number of unique people who saw this post from a sponsored product, such as ads for Page posts or sponsored stories.* ***Viral reach:*** *The number of unique people who saw this post from a story published by a friend. These stories can include liking, commenting or sharing your post, answering a question or responding to an event.*		

Table 7: Reach of EISAS announcement among the 507 CERT.PL followers on Facebook

The effects of different channels can also be neatly seen in an analysis carried out by CESICAT on referrals to the awareness materials presented on the EISAS Pilot pages of the CESICAT website (See Table 8).

Here, the staff of the General Police Department of Catalonia is clearly among the most frequent visitors of the CESICAT website and – for some reason – liked the Botnet awareness

material most. As found in the EISAS Basic Toolset study[43], the power of word of mouth as a dissemination channel for IT security awareness information should not be underestimated.

Material	Catalonia	Twitter	Google	Facebook	GPD[44]
SE Movie	102	21	174	-	-
ID Theft	102	17	15	10	10
Botnet	482	24	15	1	358
EISAS/CESICAT	47	13	8	-	-

Table 8: Referrals to EISAS Pilot awareness material presentation on CESICAT website

Figure 13 shows the clickstream from the main announcement site down to the material hosted on the LMU flash hosting server. CERT Hungary, for example, has about 4,500 visits on its homepage within the time frame of the dissemination. Of those visits, N=58 went on to the EISAS Pilot homepage and so on. Some visits to the sites hosting the materials are referred to from other channels, so the numbers on subordinate sites can be higher.

All in all, the investments of CESICAT in the presentation of EISAS on their website paid off: relative to the number of visits on the CESICAT homepage and the number of followers on Facebook, CESICAT directed the largest number of users to the EISAS awareness-raising materials.

Considerable programming effort went into implementing the online evaluation survey attached to the SE movie and the database collecting demographic data provided by respondents at the end of the ID Theft quiz, so it is worth mentioning that those two possibilities remained virtually unused by the citizens using the awareness materials.

[43] *http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-basic-toolset*

[44] *General Police Department*

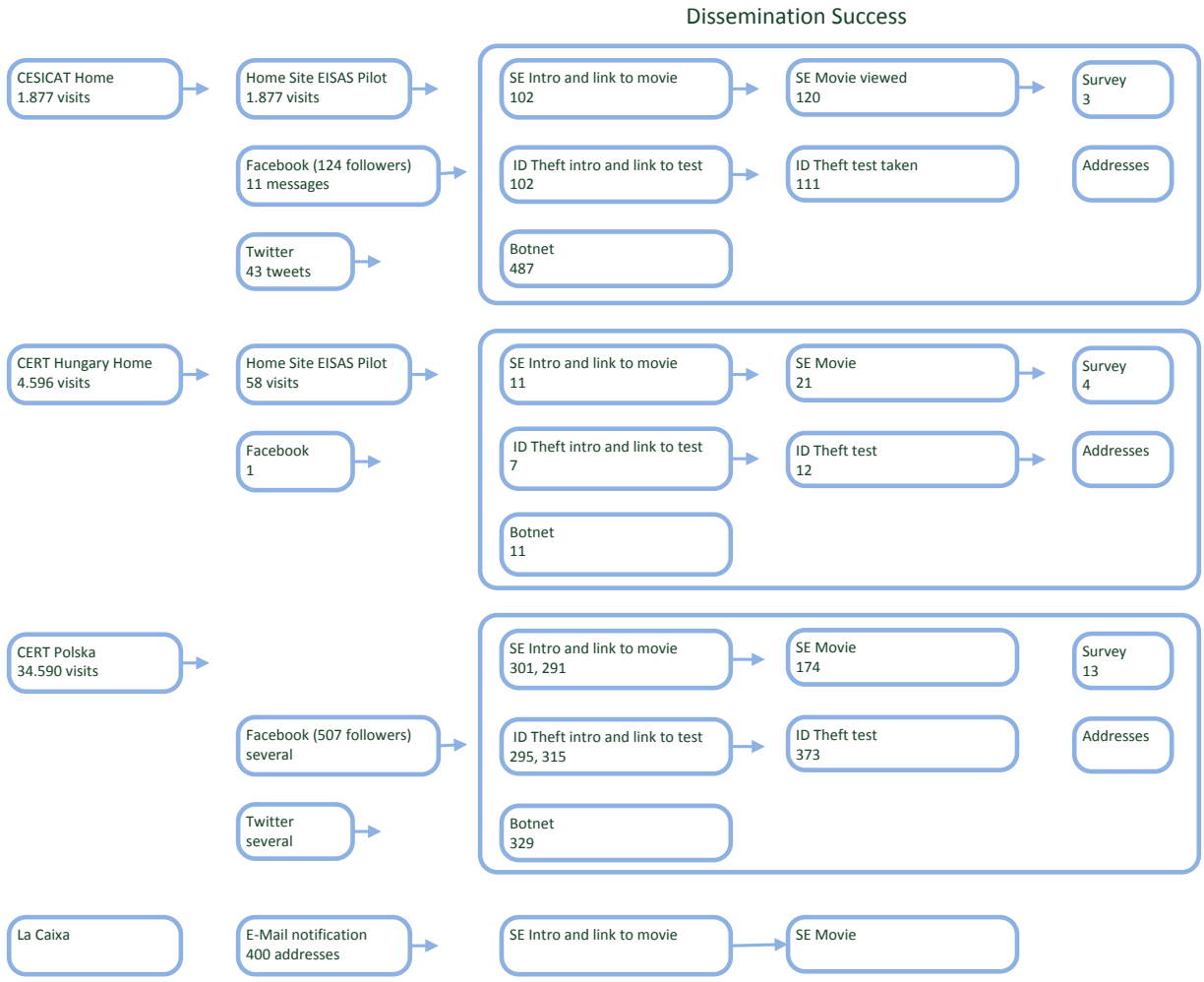


Figure 13: Clickstream graphic – from announcement to viewing the awareness material

6.2 SMEs

In awareness raising, SMEs have a definite advantage in reaching users: they know their users, know how they can be reached and thus can address them via *push* channels (e.g., email, telephone, invitation letters, magazines subscribed, informal communication, and so on).

In this pilot, la Caixa ran the dissemination campaign through targeted emails announcing the SE movie. Through an email newsletter that alerts employees twice a month of new threats and new security measures, employees were invited to see the SE material hosted on the ENISA/LMU websites.

The mail was sent out on 17 October 2012 to a list of N=400 subscribers and had N=120 views and N=86 unique views within the first two workdays after the mail newsletter was sent. This results in a reach of more than 20% of the population addressed within two days, which is significantly better than what was achieved by the other participants in the pilot, who achieved a proportional reach of about 0.2% (CERT Hungary) to 1% (CERT Poland).

CERT Poland for example also disseminated the materials only by posting alerts on its Facebook page and Twitter, so we could recalculate the proportional reach here using the base of N=507 followers and find a reach of 59% of the targeted population.

The findings are in line with what was found in the EISAS Basic Toolset 1.0. Here, one participating enterprise first published a link to the security awareness material on the enterprise security website, achieving a proportional reach of about 0.6%, and then sent out an email alert to the employees of one department, achieving a reach of 25% within one workday.

We can take two essential lessons from these outcomes:

1. Push (mail) approach results are far and away superior to pull (website) results.
2. *General interest* in the topic of IT security is the main reason people consume security-awareness messages[45].

These outcomes can lead to some speculation on if and how the general focus of security-awareness campaigns could be realigned from relying on web presentation to an awareness strategy that uses push methods. It acknowledges the fact that awareness building cannot be compared with selling a product on a website, but is a social occurrence and a process of changing knowledge, attitudes and behaviour involving the social networks of the citizens[46].

---

[45] *This is in line with what the body of learning science tells us about the factors leading to teaching success. The key factors for teaching success are (in this order): prior knowledge of the topic, interest in the topic, motivation to learn, amount of teaching, quality of teaching.*

[46] *Some concepts of importance in the context of this discussion are opinion leadership (Katz and Lazarsfeld (1955) and Straubhaar et al. (2012)) and the large body of research on the diffusion of innovations and ideas (Rogers & Rogers (2005) and Vishwanath & Barnett (2011)).*

6.3 Participants

All participants – information providers and information disseminators alike – are in the profession of IT security, so participating in this project should have "spill over effects" on other things participants do. This was invariably the case. Taking part in the project stimulated internal discussions on how to improve material production and awareness campaigns in the future. All participants agree that without the work of the information broker, the EISAS Pilot would not have been possible.

Tangible benefits for the information providers included that their materials – the Social Engineering movie and ID Theft test – were translated into four more languages (Catalá, Español, Polski, Magyar) and their names were advertised in the course of the project.

The information disseminating participants can use the material to enhance their overall information strategy. As one participant put it: "We think that the SE movie with its accompanying text is extremely valuable to demonstrate to enterprises the possibility of being subject to information theft. We can also adapt the text and create some information nuggets addressed to banks, consulting firms and other enterprises that manage important information."

7 Conclusions and recommendations

7.1 Main findings

The most important outcome of this study is that EISAS is feasible on a large scale and can be recommended for implementation throughout Europe.

With cross-border cooperation and public-private partnerships[47], the goal of the pilot was reached: six different entities in four Member States are collaborating in a joint awareness-raising campaign on an ongoing basis.

Considering the investments in time and effort of the participants (see Table 5), it becomes clear that coordination and **information brokering** between pilot actors is decisive: more than 80% of the work needed to implement EISAS in this pilot was done by the information broker.

Also, even though high-quality materials suited for collaborative dissemination are difficult to find, they are a prerequisite condition for getting information disseminators motivated to take on the workload required by getting the material online.

7.2 Lessons learned

Participating stakeholders and users considered the awareness material used in the EISAS Pilot project to be of high quality, and their impressions were favorable. Information disseminators invested significant time and effort in getting the material online, and all participants were impressed by what had been reached in this short period of time.

7.2.1 Project management

The largest proportion of work went into project management tasks. Project management here comprised more than the daily administrative details of making it possible to meet a tight schedule. It first and foremost was the exertion of “soft skills” such as maintaining participants' motivation to overcome such obstacles as working together at a distance and reassuring the participants that it was worthwhile to go on.

[47] *This puts into practice the adopted parliamentarian resolution on CIIP (12 June 2012) that “*advocates a close relationship and interaction between national private sectors and ENISA to interface the National/Governmental CERTs with the development of the European Information Sharing and Alert System (EISAS)*”; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0167+0+DOC+XML+V0//EN*

7.2.2 Programming

The expenditures necessary for programming seemed surprisingly high. Given that web programming is immature compared to systems programming, one should be prepared for this expenditure when adapting and localising awareness materials.[48]

Because the programmer has to learn how the application works before even starting to adapt and localise the awareness material, a decentralised approach seems too ineffective.

Furthermore, it is neither an efficient nor an effective use of disseminator time if the task of understanding how an application works had to be repeated by every information disseminator.

7.2.3 Dissemination

From the point of view of successfully managing an international cross-border security awareness campaign, the project went very well. However, some participants felt that the reach fell short of what would be expected, given the efforts necessary to get the materials online and distributed. Indeed, based on the expenditures of 250 person-days for a reach of about 1,500 citizens and SME users, getting IT security awareness information to the end user is obviously not inexpensive using this approach.

However, the expected reach was achieved in the project, based on what is known from unpublished data of other awareness campaigns that used material similar to that of the EISAS Pilot.

7.2.4 Human factors

One important lesson learned from the project is that IT security information is not as attractive to ordinary users as IT security specialists might hope it to be. The point is that many non-security considerations go into security decisions, and security considerations are secondary by default. In an essay titled "Nonsecurity Considerations in Security Decisions", Bruce Schneier[49], one of the world's most renowned security specialists, depicts that even for owners of assets of worth, security is only a minor consideration in a security decision.[50]

Any IT security professional who expects that it is only a matter of time until the users will learn that it is important to go for IT security and protect oneself will come across another

---

[48] *"All programmers are optimists. Perhaps this modern sorcery especially attracts those who believe in happy endings and fairy godmothers. Perhaps the hundreds of nitty frustrations drive away all but those who habitually focus on the end goal. Perhaps it is merely that computers are young, programmers are younger, and the young are always optimists. But however the selection process works, the result is indisputable: 'This time it will surely run,' or 'I just found the last bug'. So the first false assumption that underlies the scheduling of systems programming is that all will go well, i.e., that each task will take only as long as it 'ought' to take" (Brooks 1995, p. 14).*

[49] *http://www.schneier.com/*

[50] *See article by Bruce Schneier (2007) and the large body of research on naturalistic decision making (Todd & Gigerenzer (2001), Zsambok & Klein (1997)).*

obstacle for getting security-awareness messages to users: IT security is an abstract concept that is difficult to learn.

For a typical everyday user of IT equipment and services, a decision in favour of IT security measures, such as immediately applying a patch or using a secure but complicated password, does not have a tangible outcome to that user's daily operations, and usually the user perceives no threat, so it is easy to ignore such IT security measures. In contrast, the reward for a decision in favor of IT security measures that actually detract from the task at hand only carries a vague perception that some abstract danger would be averted.

In a normal learning situation, behaviour is formed by positive reinforcement. If we do something right, we get rewarded. In the case of IT security decisions, the positive reinforcement is that there is a lower probability that some abstract danger would become a reality.

If this danger manifests itself as harm to the user – which is rarely the case or goes unnoticed because the harm incurred by one user on his device actually hits another user – the harm done can surface days, weeks or months after the wrong IT security decision.

This makes learning from negative consequences of wrong decisions in IT security extremely difficult, with the exception of spectacular catastrophic failures.

Awareness-raising professionals can benefit from methods that push learning of proper IT security behaviour to the user. Awareness raising cannot wait until the user recognises what is at stake and starts changing his behaviour out of insight and motivation. Promising new approaches that employ web-based embedded training and micro games are being developed that are worthy of note and give reasonable hope[51].

Bearing in mind the important role that human factors play in the effectiveness of awareness raising and security training, a more psychological and educational orientation is an important component in helping EISAS to achieve sustained success.

7.2.5 Information broker

Clearly, the information-providing and information-disseminating participants could never have come together without an information broker. The information broker role entails the necessary big task blocks of project management, programming and documentation – tasks that if left to the information providers and, most notably, the information disseminators would have overstrained their initially allocated time budgets.

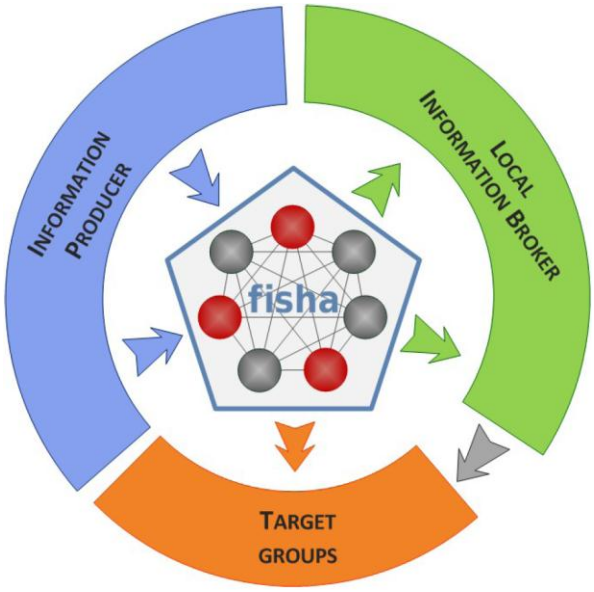
[51] *See Jakobsson (2007) and Hong (2012).*

7.3 Next steps

7.3.1 NISHA, the promising sharing infrastructure

Following the recommendations of the EISAS Roadmap, a consortium was developed in 2009–2011, namely, the Framework for Information Sharing and Alerting (FISHA), to focus on the technical aspects of EISAS. In 2012, a new project was established to further the development of the FISHA project – the Network for Information Sharing and Alerting[52] (NISHA) project.

NISHA is designed as a peer-to-peer (P2P) network at the European level, operated by core nodes (actors) and used by local nodes. The information flow model used by the NISHA prototype conceives a node who runs a local web portal that provides information for end users, generates new information, increases the value of information by translating the information into other languages, tailors the information to the constraints of various dissemination channels (e.g., website, Facebook, Twitter, email newsletter, and so forth) and to the characteristics of the target groups (i.e., various subgroups of citizens and different types of SMEs).



NISHA uses a terminology slightly different from the terminology used in the EISAS Pilot. NISHA refers to the "local information broker" as used in EISAS as the role of the "information disseminator" and it also includes channels such as print and broadcast media, big portals, and so on.

NISHA's information broker is a local entity that takes worthwhile information from original information producers and does all the information processing work described in the report to make the original information usable for distribution by the local information disseminators.

Without doubt, this sharing and disseminating infrastructure is a promising technical tool to support upcoming exchanges and enhance cooperation among future EISAS stakeholders.

7.3.2 Fostering Cooperation

The EISAS Pilot clearly shows that participants willing to provide information, be it through the NISHA infrastructure or not, have to be supported by some entity that takes over the task of

[52] *For more on FISHA and NISHA projects, see http://fisha-project.eu/; NISHA is being carried out by the four project partners, PTA/CERT-Hungary, NASK/CERT Polska, University of Gelsenkirchen/Institute for Internet Security, and FCCN / CERT.PT.*

information post-processing (from the point of view of the information provider) and the task of information pre-processing (from the point of view of the information disseminator).

Cooperation means communication among willing humans to help each other with providing the human intelligence needed to make information attractive and useful to diverse target groups with diverse channels.

At least for the start-up phase, the NISHA infrastructure should be supported by some information brokering entity – albeit centralized or cooperatively organised – that helps

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

The outcomes of the EISAS Pilot show that a situation in which dissemination and consumption of IT security information runs by itself is highly improbable, at least in the early phases of community building.

8 Annex I: References

Ajzen, Icek, Fishbein, Martin, Heilbronner, Robert L. (1980), "Understanding Attitudes and Predicting Social Behavior", Prentice Hall.

Brooks, Frederick P. (1995), "The Mythical Man Month: Essays on Software Engineering", Anniversary Edition, Addison Wesley.

Dourish, Paul, Grinter, Rebecca E., Delgado de la Flor, Jessica, Joseph, Melissa (2004), "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem", Personal Ubiquitous Computing, 8, 391-401.

ENISA (2011a), European Month of Network and Information Security for All – A Feasibility Study
http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2011/europeansecuritymonth/at_download/fullReport.

ENISA (2011b), "EISAS Basic Toolset 1.0. Feasibility Study of Home Users' IT Security", http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-basic-toolset.

ENISA (2012), “Deployment of Baseline Capabilities of National/Governmental CERTs”,

Fishbein, Martin (1975), "Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research", Longman Higher Education.

Guarascio, Francesco (2011), "Can the EU close Europe's digital divide?", http://www.publicserviceeurope.com/article/711/can-the-eu-close-europes-digital-divide.

Hong, Jason (2012), "The State of Phishing Attacks", Communications of the ACM, 55 (1), 74-81.

Jakobsson, Markus (2007), "The Human Factor in Phishing", in: Privacy and Security of Consumer Information '07, 2007, downloadable at http://markus-jakobsson.com/papers/jakobsson-psci07.pdf.

Jarvenpaa, Sirkka L., Knoll, Kathleen, Leidner, Dorothy E. (1998), "Is Anybody Out There? Antecedents of Trust in Global Virtual Teams", Journal of Management Information Systems, 14 (4), 29-64.

Jarvenpaa, Sirkka, Leidner, Dorothy E. (1999), "Communication and Trust in Global Virtual Teams", Organization Science, 10 (6), 791-815.

Katz, Elihu, Lazarsfeld, Paul (1955), "Personal Influence: The Part Played by People in the Flow of Mass Communications", Transaction Publishers 2005.

Kitten, Tracy (2012), "New Strategies to Fight Phishing. As the Fraud Threat Grows, Battle Plans Change", http://www.bankinfosecurity.com/p_print.php?t=a&id=4635.

Krug, Steve (2005), "Don’t Make Me Think! A Common Sense Approach to Web Usability", New Riders.

Nielsen, Jakob (1999), "Designing Web Usability: The Practice of Simplicity," New Riders.

Olson, Gary M., Olson, Judith, S. (2000), "Distance Matters", Human-Computer Interaction, 15 (2-3), 139-178.

Rogers, Everett M., Rogers, E. (2005), "Diffusion of Innovations", Free Press.

Samarajiva, Rohan (2005), "Mobilizing Information and Communication Technologies for Effective Disaster Warning: Lessons from the 2004 Tsunami", New Media & Society, 7(6), 731-747.

Schneier, Bruce (2007), "Nonsecurity Considerations in Security Decisions", IEEE Security & Privacy, May 2007, 88

Straubhaar, Joseph, LaRose, Robert, Davenport, Lucinda (2012), "Media Now: Understanding Media, Culture, and Technology", Wadsworth.

Todd, P., and Gigerenzer, G. (2001), “Putting Naturalistic Decision Making into the Adaptive Toolbox”, Journal of Behavioral Decision Making, Vol. 14, 381-383.

Van Deursen, Alexander, Van Dijk, Jan (2010), "Internet Skills and the Digital Divide", New Media & Society, 13 (6), 893-911

Van Dijk, Jan (2005), "The Deepening Divide Inequality in the Information Society", Sage 2005.

Vishwanath, Arun, Barnett, George A. (2011), "The Diffusion of Innovations", Peter Lang Publishing.

Zipf, George Kingsley (1949), "Human Behavior and the Principle of Least Effort: An Introduction to Human Ecology", Martino Fine Books 2012, reprint of the original 1949 edition.

Zsambok, C.E. and Klein, G (1997) “Naturalistic Decision Making”, Lawrence Erlbaum Associates.

9 Annex II: Abbreviations

BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der informationstechnik)
CERT	Computer Emergency Response Team
CESICAT	Information Security Centre of Catalonia
CIIP	Critical Information Infrastructure Protection
CSO	Chief security officer
DDoS	Distributed Denial of Service
DG HOME	Directorate General for Home Affairs
DTAG	Deutsche Telekom AG
EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
FIRST	Forum of Incident Response and Security Teams
FISHA	Framework for Information Sharing and Alerting
ICT	information and communications technologies
ID	identity
IS	Information Security
IT	Information Technology
NASK	Research and Academic Computer Network (Poland)
n/g	national/governmental
NGO	non-governmental organisation
NIS	Network and Information Security
NISHA	Network for Information Sharing and Alerting
NorSIS	Norwegian Centre for Information Security
P2P	peer-to-peer
PC	personal computer

PPP	public-private partnership
SME	Small and medium enterprise
WARP	Warning, Advice, and Reporting Points

10 Annex III: EISAS Pilot Participants

Table 9: Participants

Entity	Contact Person	…
Deutsche Telekom AG	Josef Paulik	http://www.telekom.com/
NorSIS	Tore Orderløkken	http://www.norsis.no/
CERT Hungary	Bence Birkás	http://www.cert-hungary.hu/
CERT Poland	Katarzyna Gorzelak	http://www.cert.pl/
CESICAT	Ivan Monforte Fugarolas	https://www.cesicat.cat/
la Caixa	Raúl Amigorena Eguíluz	http://www.lacaixa.es

Table 10: Information brokers

Entity		
Translation	Hungarian Polish	http://www.doctusoft.com/ http://www.star-ts.com
LMU IT Infrastructure	Hans-Peter Klein Christian Giese	http://www.lmu.de/ http://codeandconcept.com/en/
Programming	Emanuel Seibold Erik Ebell Thomas Ledwon	http://www.lmu.de/ http://codeandconcept.com/en/ http://www.lmu.de/
Project Management	Werner Degenhardt Romain Bourgue	http://www.lmu.de/ http://www.enisa.europa.eu/
Networking and Contacts	Werner Degenhardt Klaus Kristensen Romain Bourgue	http://www.lmu.de/ http://www.i-trust.dk/ http://www.enisa.europa.eu/
Report Writing	Werner Degenhardt Romain Bourgue	
SME Consulting	Rainer Seidlitz	http://www.tuev-sued.de/management_systeme/it-dienstleistungen

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