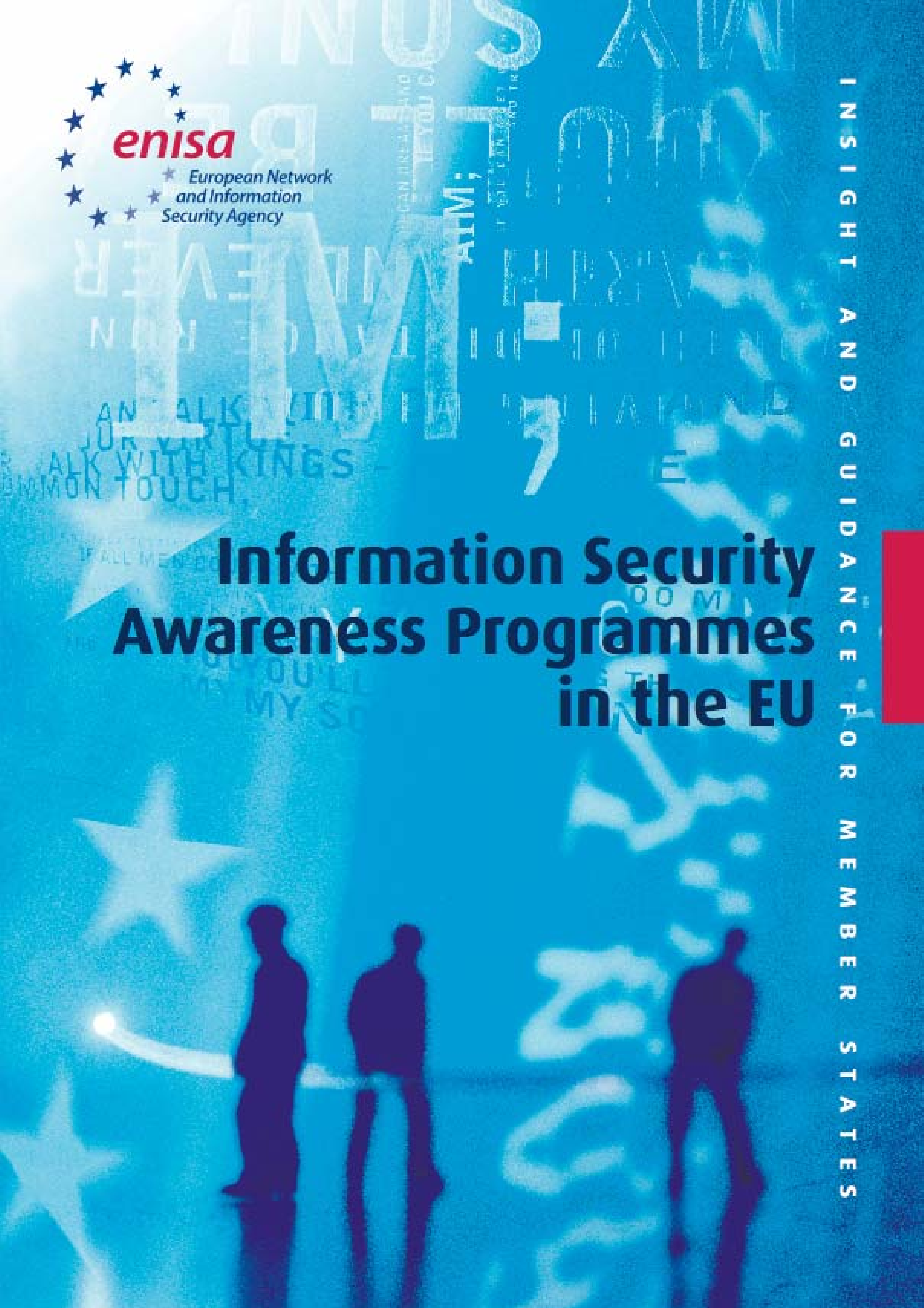


enisa
European Network
and Information
Security Agency

Information Security Awareness Programmes in the EU

INSIGHT AND GUIDANCE FOR MEMBER STATES

enisa
European Network
and Information
Security Agency

Information Package 2006

Information Security Programmes in the EU:

Insight and Guidance for Member States

September 2006

Legal Notice

By the European Network and information Security Agency (ENISA).

Notice must be taken that information contained in this Information Package has been compiled by ENISA staff also on the basis of information that has been supplied to ENISA by appropriate organisations and bodies within the EU Member States or is publicly available. This Information Package does not necessarily represent state-of the-art and it might be updated from time to time.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contains in this publication. ENISA is not responsible for the content or the external web sites referred to in this publication.

Table of Contents

Summary

The uses of Information Communication Technology (ICT) continue to increase in all Member State countries. As in the past, the benefit to businesses and citizens through increased coverage and advances in technology has been countered by an increasing number of information security breaches. The current environment therefore still demands that Member States continue to promote and develop a “culture of security”.

The adage that “you are only as strong as your weakest link” is prevalent in today’s IT landscape and it is the human element that is still a critical factor when implementing any effective and robust security framework. The European Network and Information Security Agency (ENISA) and the Member States are continuing their efforts to positively influence the public’s behaviour towards information security, changing the mindset of the human element in order to achieve greater self-awareness.

This Information Package details the awareness raising initiatives either undertaken or underway within Member States. The information has been compiled based on the responses from the countries to the ENISA Questionnaire. This information has been supplemented by interviews, research and additional material. It is envisaged that the details contained be used to help disseminate practical information of good practices as well as offer an opportunity to monitor the progress in the national approaches to addressing information security awareness.

Analysing the initiatives and efforts by Member States, several trends and commonalities have been identified with the work done to date:

- The total number of awareness raising initiatives in the EU has slightly risen over the last year
- Two-thirds of awareness programmes conducted have been run in the north of Europe
- As in the past, the difference in nature and number of awareness initiatives derives from the different levels of information security understanding and culture within the countries
- Almost every programme in Member State countries targeted the SME and Home User groups
- Awareness raising collaboration is growing with Internet Service Providers (ISPs)
- As in the past, phishing, spam and protection through firewalls are the main themes that are covered - in the last year, almost all awareness initiatives have included identity theft as a topic

- Awareness raising subjects that are growing in coverage include the use of mobile devices and WiFi
- Websites and training remain the most used communication channels to deliver the message as part of any awareness raising initiative
- Media is still primarily being used as a channel of communication, and not as a target group. Responses from Member States detailed in the Information Package confirm this

When analysing the most effective programmes that have been executed, and based on good practice methodology from ENISA, it is possible to identify several key pre-requisites and actions that are required for a successful awareness raising initiative:

- The message delivered has to be appealing and perceived as “of value” to the target group - the audience should be properly evaluated with interests, needs and knowledge identified
- Communication channels should be analysed to identify then use the optimal delivery mechanisms - preferred communication channels per target group should be understood and utilised
- Public-private partnerships should be used to leverage synergies to help make sure that the initiative has the resources and expertise to deliver the right message to the right people using the most effective channels
- Multipliers such as teachers and the Media should be used to help increase the scope and coverage of any awareness raising initiative
- Metrics and KPIs should be used to measure the effectiveness of an initiative – lessons learnt through analysis of quantitative and qualitative data can be used to help improve future campaigns

Introduction

The digital information age that we live and work in continues to provide many opportunities for businesses and citizens. However, the further development and user adoption of Information Communication Technologies (ICTs) still comes with vulnerabilities. Businesses and citizens are still at risk of dangers such as information security breaches. Analysts still report that the human component in any information security framework is the weakest link, implying that changes in user perception or organisational culture are still required.

As part of the 2005 Work Programme, ENISA delivered the Information Package "Raising Awareness in Information Security – Insight and Guidance for Members States".[1] The document and CD application created were designed to provide an analysis of successful practices adopted by EU Member States, and to highlight measures already underway in the awareness raising field. This year, to continue to facilitate and help raise awareness and promote good practices, the Agency has revisited the Information Package 2005 in order to detail current trends and the progress made in the Member States.

[1] See full text of the "Information Package: Raising Awareness in Information Security – Insight and Guidance for Members States" at http://www.enisa.europa.eu/pages/05_01.htm

Scope

At the end of 2005, ENISA and the OECD explored how the two organisations could co-operate in the area of information security, with particular attention to raising awareness in this field.

A review of the effectiveness of awareness raising activities highlighted a need for a more strategic approach. A more effective strategy would be to ensure that campaign results and general awareness information would be provided to one organisation only. Thus the Agency and the OECD recognised the long term need for collaboration and the avoidance of duplication of efforts. This approach is aimed at improving the efficiency of gathering information with regards to awareness raising initiatives, with a view to ensure the effectiveness of the anticipated results.

On this basis, ENISA developed a questionnaire which was focused on awareness raising matters which had not been explored in detail by either the ENISA Information Package 2006 or the “OECD questionnaire on practical initiative to promote a culture of security”. This included gathering details for two additional target groups: Internet Service Provider (ISP) and Local Government. The questionnaire (sent to the Member States and the Permanent Stakeholder Group (PSG)[2]), was aimed at extracting pertinent information in a way that was suitable to the responder. Mainly focused on the public sector, the questionnaire also provided for input from the private sector. Narrative style questions and structure allowed for responders to control the format and size of the response without necessarily confining themselves. Whilst the priority of the questionnaire was the collection of good practice material, the approach adopted also allowed responders the opportunity to present awareness related initiatives as they perceive them themselves.

This information has been supplemented by interviews, research and additional material.

The purpose of the Information Package 2006 is therefore to provide an overview of the EU awareness programmes. The overview primarily consists of the text which has been supplied by the Member States or by other organisations. The Agency has also constructed good practice recommendations as well as offering guidance on running awareness raising campaigns. This includes information on metrics and key performance indicators (KPIs). A roadmap has also been created to show a holistic progression of awareness raising initiatives.

[2] The Executive Director of ENISA has established the Permanent Stakeholders’ group on 28th February 2005. The PSG is composed of experts representing the relevant stakeholders, such as Information and Communication Technologies industry, consumer groups and academic experts in network and information security. The PSG advises the Executive Director in the performance of his/her duties under this Regulation, in drawing up a proposal for the Agency’s work programme and in ensuring communication with the relevant stakeholders on all issues related to the work programme.

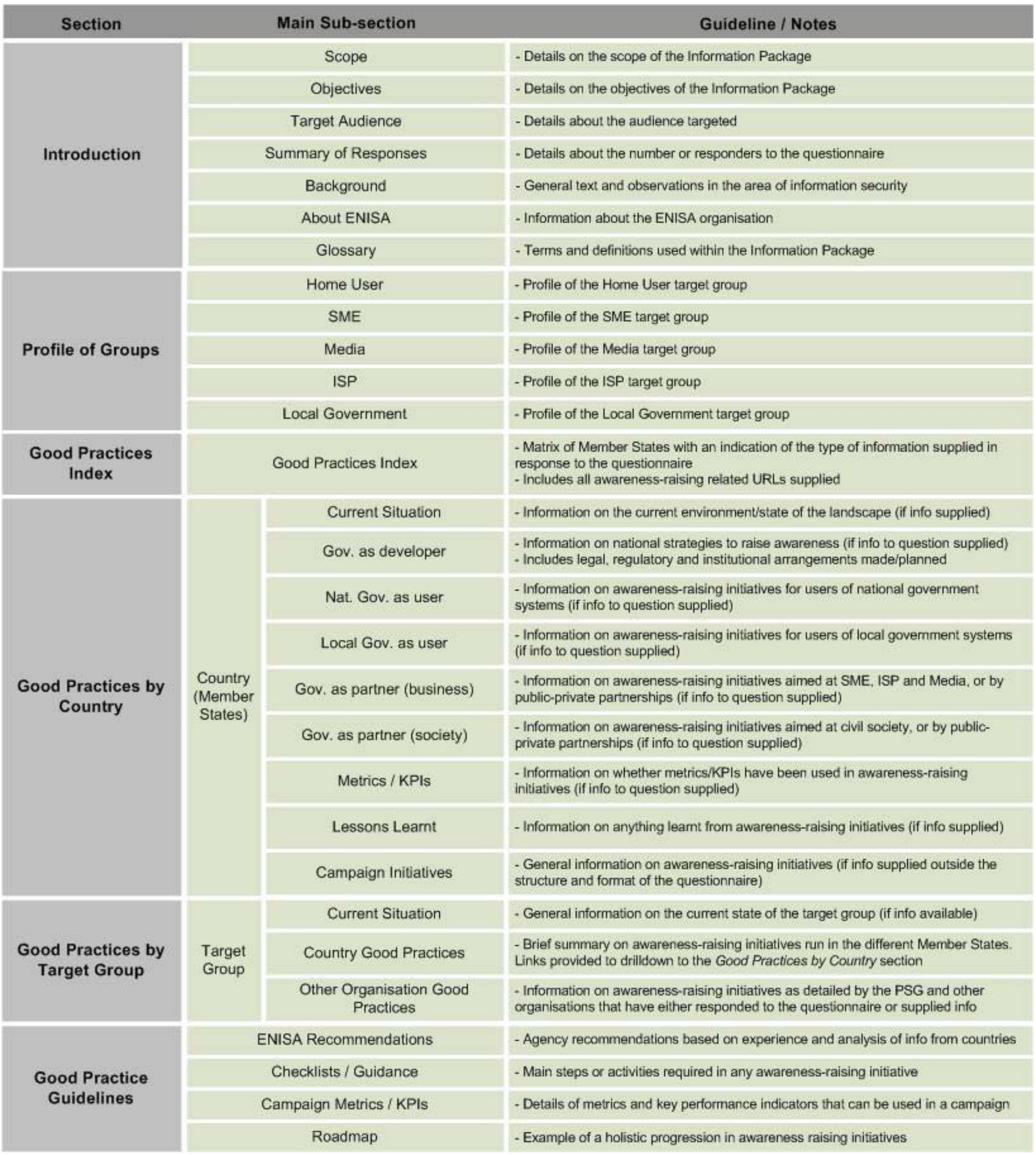
This Information Package should not be seen as a comprehensive source of information of all information security awareness raising initiatives that have been undertaken; the Information Package is only as comprehensive as the level of detail provided by the Member States, organisations and bodies. This package is also not a guideline to the types or content of messages that should be used as part of any awareness raising initiative; neither does it serve as a technical guideline to information security standards or solutions.

Objectives

The ENISA Information Package 2006 is intended to:

- Detail and help monitor the progress made in national approaches to awareness raising
- Provide an inventory of good practices from the Member States and other organisations
- Provide general recommendations on good practices in awareness raising
- Provide good practice material that can be customised and presented to the Member States to help facilitate their work on awareness raising
- Offer guidance on running effective awareness raising campaigns and on how to use metrics and KPIs to monitor the performance of initiatives
- Offer an example approach to conducting an awareness raising campaign
- Contribute to the development of an information security culture in Member States

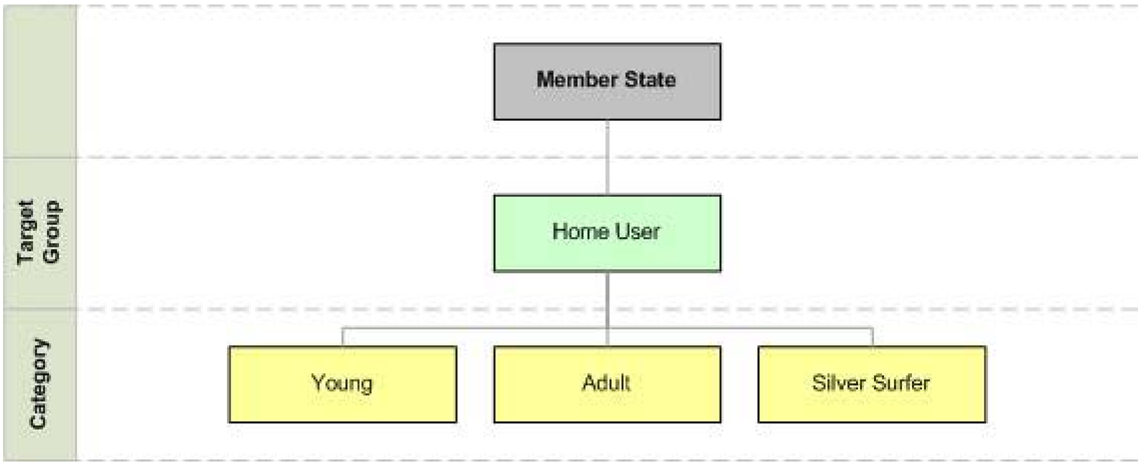
To help achieve these objectives and to easily disseminate the information, the following structure has been adopted:

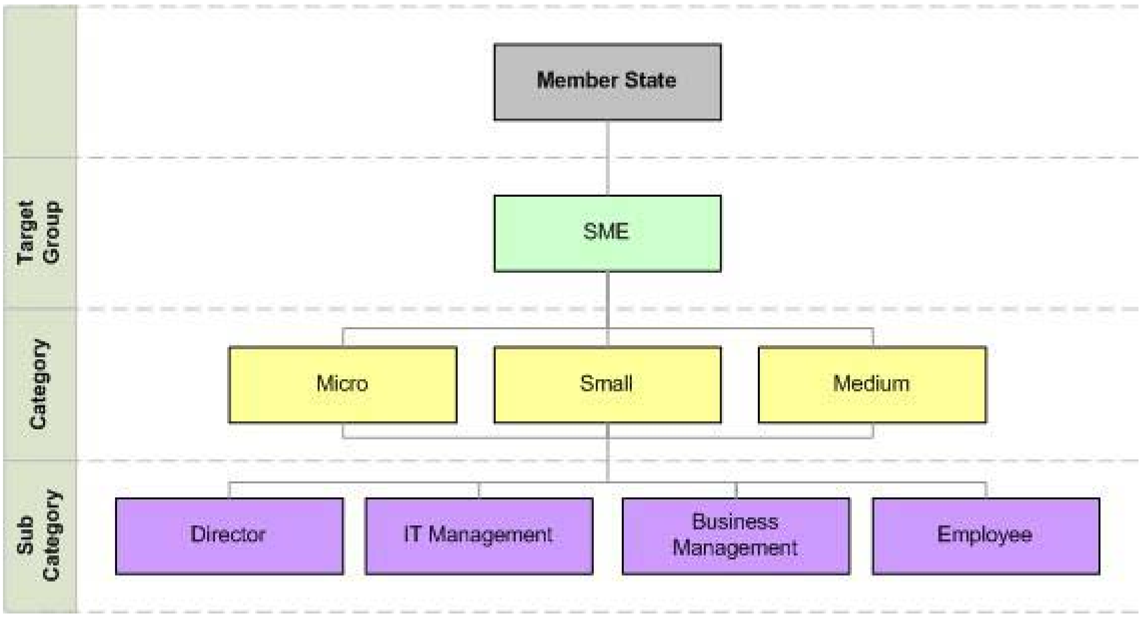


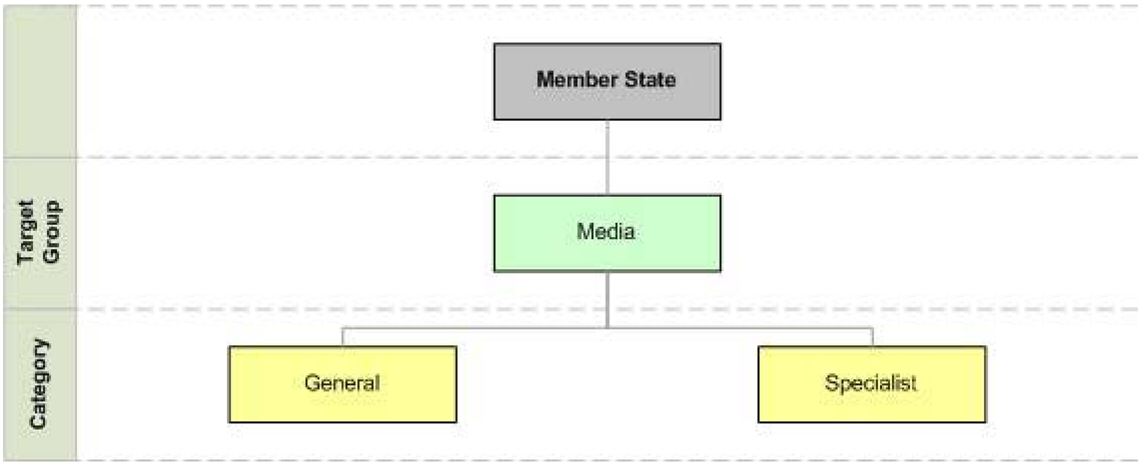
Section	Main Sub-section		Guideline / Notes
Introduction	Scope		- Details on the scope of the Information Package
	Objectives		- Details on the objectives of the Information Package
	Target Audience		- Details about the audience targeted
	Summary of Responses		- Details about the number or responders to the questionnaire
	Background		- General text and observations in the area of information security
	About ENISA		- Information about the ENISA organisation
	Glossary		- Terms and definitions used within the Information Package
Profile of Groups	Home User		- Profile of the Home User target group
	SME		- Profile of the SME target group
	Media		- Profile of the Media target group
	ISP		- Profile of the ISP target group
	Local Government		- Profile of the Local Government target group
Good Practices Index	Good Practices Index		- Matrix of Member States with an indication of the type of information supplied in response to the questionnaire - Includes all awareness-raising related URLs supplied
Good Practices by Country	Country (Member States)	Current Situation	- Information on the current environment/state of the landscape (if info supplied)
		Gov. as developer	- Information on national strategies to raise awareness (if info to question supplied) - Includes legal, regulatory and institutional arrangements made/planned
		Nat. Gov. as user	- Information on awareness-raising initiatives for users of national government systems (if info to question supplied)
		Local Gov. as user	- Information on awareness-raising initiatives for users of local government systems (if info to question supplied)
		Gov. as partner (business)	- Information on awareness-raising initiatives aimed at SME, ISP and Media, or by public-private partnerships (if info to question supplied)
		Gov. as partner (society)	- Information on awareness-raising initiatives aimed at civil society, or by public-private partnerships (if info to question supplied)
		Metrics / KPIs	- Information on whether metrics/KPIs have been used in awareness-raising initiatives (if info to question supplied)
		Lessons Learnt	- Information on anything learnt from awareness-raising initiatives (if info supplied)
		Campaign Initiatives	- General information on awareness-raising initiatives (if info supplied outside the structure and format of the questionnaire)
Good Practices by Target Group	Target Group	Current Situation	- General information on the current state of the target group (if info available)
		Country Good Practices	- Brief summary on awareness-raising initiatives run in the different Member States. Links provided to drilldown to the *Good Practices by Country* section
		Other Organisation Good Practices	- Information on awareness-raising initiatives as detailed by the PSG and other organisations that have either responded to the questionnaire or supplied info
Good Practice Guidelines	ENISA Recommendations		- Agency recommendations based on experience and analysis of info from countries
	Checklists / Guidance		- Main steps or activities required in any awareness-raising initiative
	Campaign Metrics / KPIs		- Details of metrics and key performance indicators that can be used in a campaign
	Roadmap		- Example of a holistic progression in awareness raising initiatives

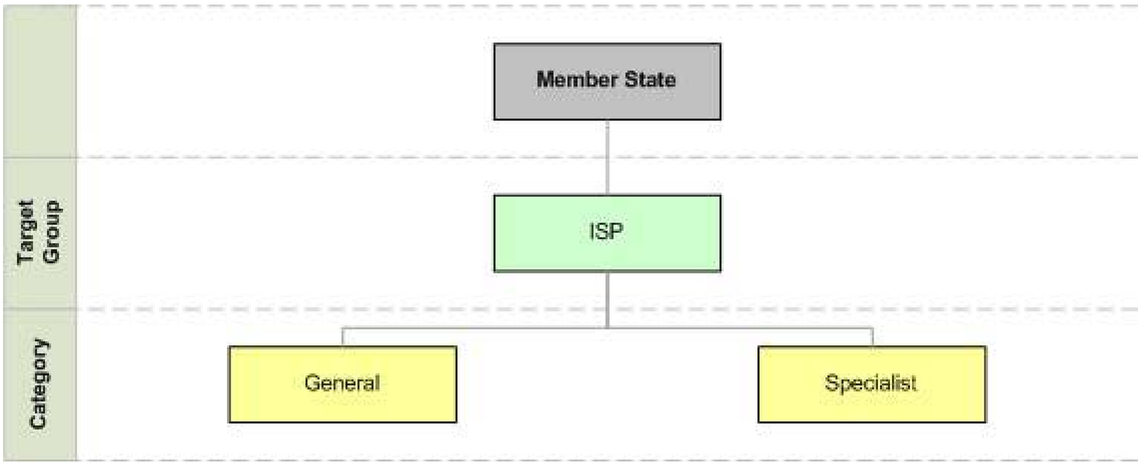
Target Audience

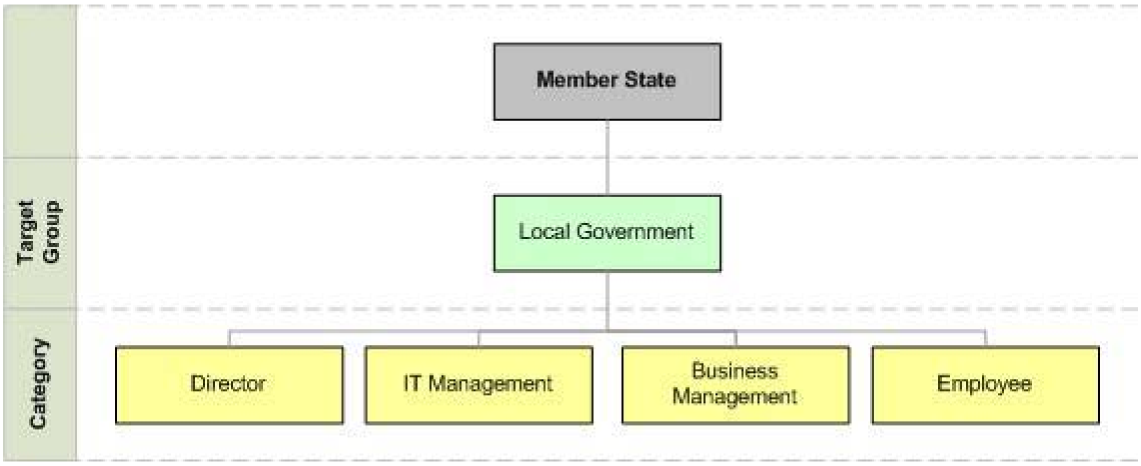
The Information Package 2006 is aimed specifically at Member States for use when conducting awareness raising campaigns. The focus is on five target groups: Home User, Small and Medium Enterprise (SME), Media, Internet Service Provider (ISP) and Local Government. Descriptions on each group can be found in the *Profile of Groups* section. Graphically, these five target groups can be illustrated as follows:











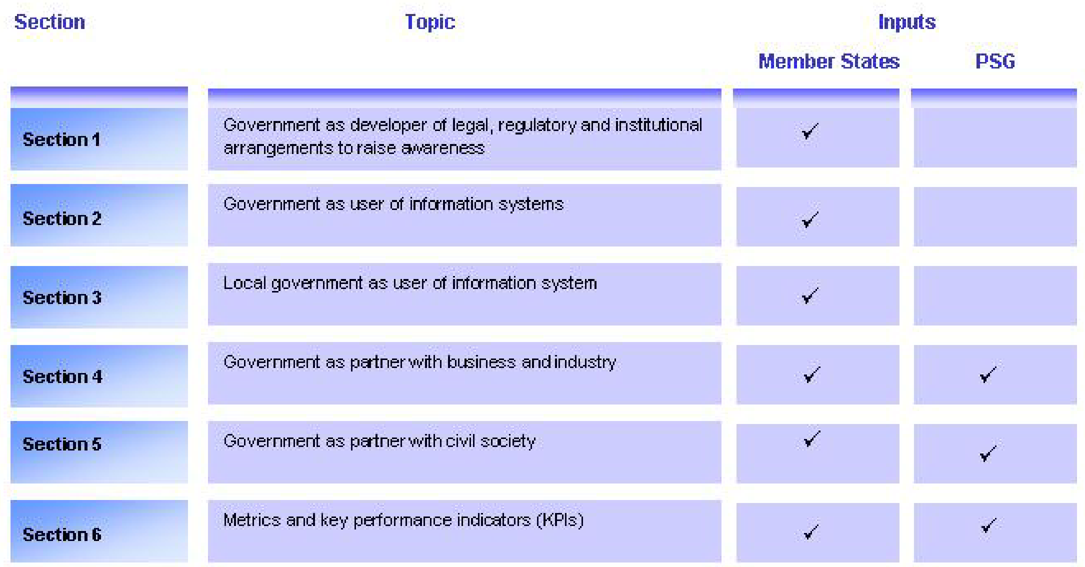
As the most essential ingredient of any successful campaign is to ensure that the communication channel used and message conveyed specifically meet the needs, interests and knowledge of those targeted, this Information Package will look to focus on these five selected groups.

Summary of Responses

The questionnaire used for the Information Package 2006 was sent out to:

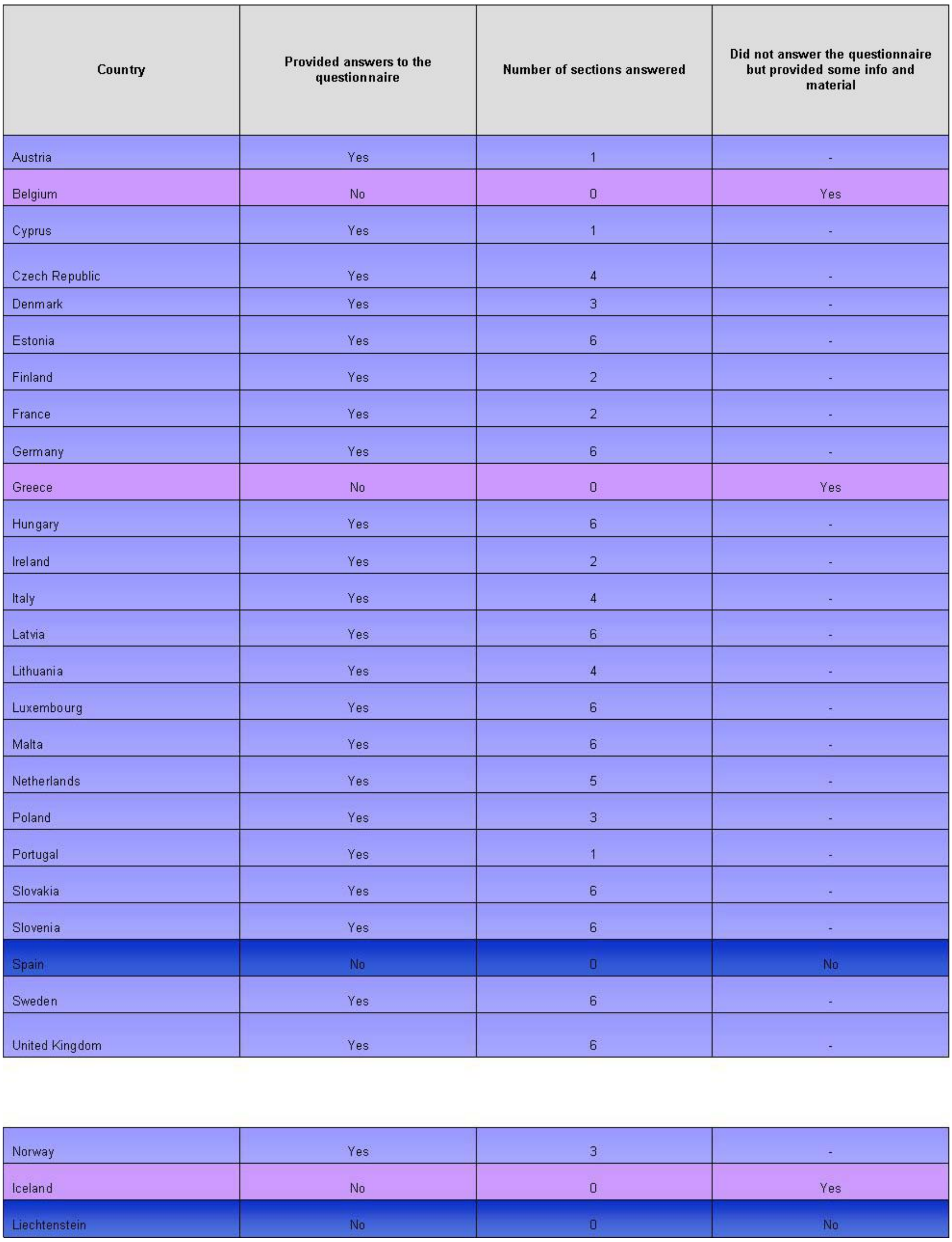
- 28 Member State countries: the 25 EU members and the 3 EEA members
- The ENISA PSG
- Private sector organisations and various other bodies

The diagram below shows which sections of the questionnaire were required to be filled in by either the Member State or the PSG:



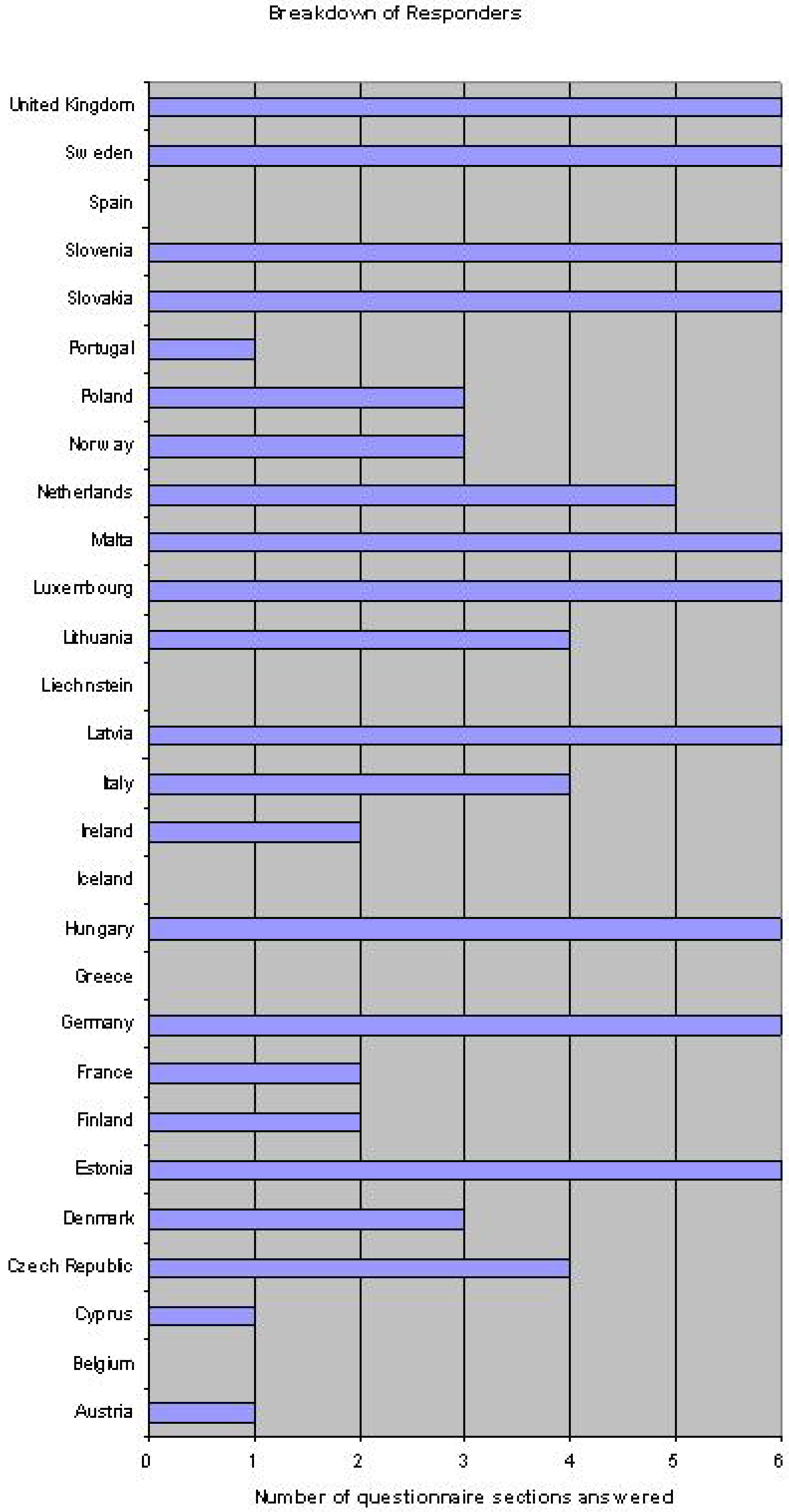
Section	Topic	Inputs	
		Member States	PSG
Section 1	Government as developer of legal, regulatory and institutional arrangements to raise awareness	✓	
Section 2	Government as user of information systems	✓	
Section 3	Local government as user of information system	✓	
Section 4	Government as partner with business and industry	✓	✓
Section 5	Government as partner with civil society	✓	✓
Section 6	Metrics and key performance indicators (KPIs)	✓	✓

The following table indicates which Member State countries answered the section questions in the ENISA questionnaire and which ones sent additional or supplementary information:

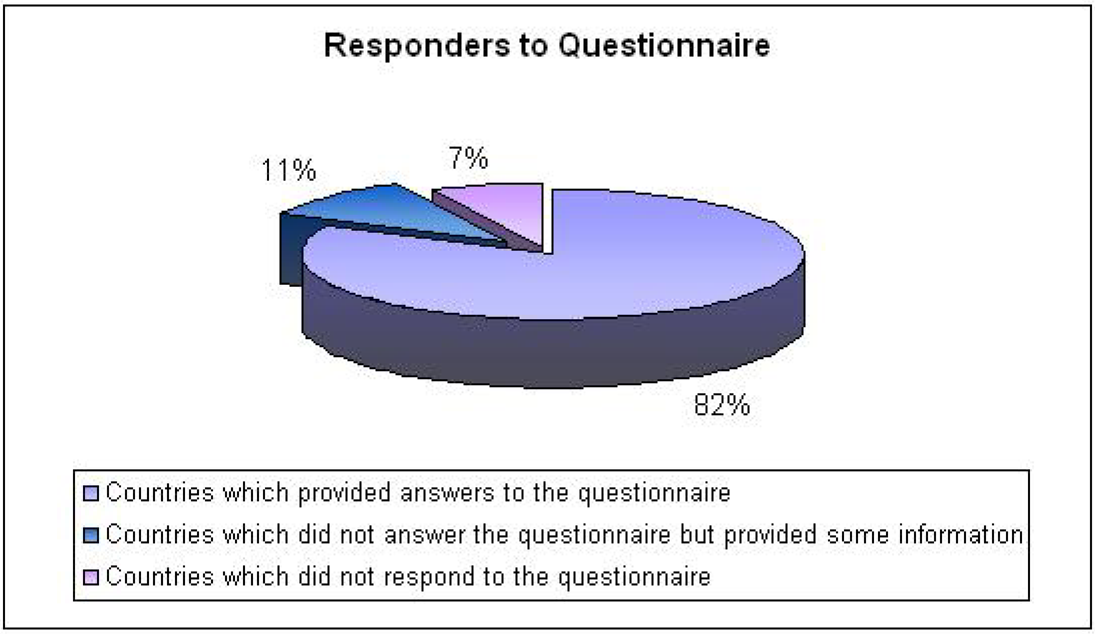


Country	Provided answers to the questionnaire	Number of sections answered	Did not answer the questionnaire but provided some info and material
Austria	Yes	1	-
Belgium	No	0	Yes
Cyprus	Yes	1	-
Czech Republic	Yes	4	-
Denmark	Yes	3	-
Estonia	Yes	6	-
Finland	Yes	2	-
France	Yes	2	-
Germany	Yes	6	-
Greece	No	0	Yes
Hungary	Yes	6	-
Ireland	Yes	2	-
Italy	Yes	4	-
Latvia	Yes	6	-
Lithuania	Yes	4	-
Luxembourg	Yes	6	-
Malta	Yes	6	-
Netherlands	Yes	5	-
Poland	Yes	3	-
Portugal	Yes	1	-
Slovakia	Yes	6	-
Slovenia	Yes	6	-
Spain	No	0	No
Sweden	Yes	6	-
United Kingdom	Yes	6	-
Norway	Yes	3	-
Iceland	No	0	Yes
Liechtenstein	No	0	No

The chart below shows a breakdown of the number of sections answered in the questionnaire by Member State:


Breakdown of Responders
United Kingdom
Sw eden
Spain
Slovenia
Slovakia
Portugal
Poland
Norw ay
Netherlands
Malta
Luxembourg
Lithuania
Liechnstein
Latvia
Italy
Ireland
Iceland
Hungary
Greece
Germany
France
Finland
Estonia
Denmark
Czech Republic
Cyprus
Belgium
Austria
0
1
2
3
4
5
6
Number of questionnaire sections answered

The following chart shows the overall summary of Member State responses:



Background

Information Security can be defined as the protection of information from various threats in order to ensure personal or work related activities can be completed.

Information Security breaches or threats can come in multiple forms. Some of these include:

- Physical theft of ICT's containing sensitive or important information
- Malicious code executed on a computer
- Hardware or software failures
- Unauthorised access or inappropriate usage
- Network disruptions
- Identity fraud

These breaches can manifest themselves in various ways, for example:

- Loss of data due to malware or theft
- Poor performance due to malware or hardware and software failures
- Unsolicited emails (spam) due to inappropriate usage
- Financial costs due to lost funds as a result of identity fraud, social engineering or downtime to systems due to network disruptions

"The threats within"[3] report by McAfee notes that amongst 1500 professional workers in 6 European cities:

- Nearly a quarter of all European professional workers use a company laptop to access the Internet at home.- this is despite 61%having a very limited knowledge about IT security
- Over half of European professional workers own devices or gadgets which they connect to the office PC/network - a quarter of these connect them to the office PC every day
- 62% say they don't have a clue about IT Security or have very limited knowledge

The Information Security Breaches Survey 2006 commissioned by the United Kingdom's Department of Trade and Industry (DTI), states that it is widely accepted that the vast majority of security breaches are the result of a human error rather than technology flaws. Assuming that the majority of information security incidents are a result of human error, then it is important to understand the potential reasons why they occur in an effort to improve the situation. Taking into account research and information collected in surveys, some of the reasons include the fact that:

- Users of ICT's are poorly trained and in general have poor security awareness

[3] Refer to the_threats_english.pdf

- People are aware of some information security issues but as users of ICT's they make poor decisions
- There are people that are malicious by nature and look to deliberately expose the organisation to risk
- People are not necessarily motivated to perform at the required levels needed for secure actions

The OECD Guidelines for the Security of Information Systems and Networks state that "Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks." The Guidelines also emphasise that citizens need to know "… good practices that they can implement to enhance security". Organisations must implement appropriate programmes to develop such awareness and knowledge, and must ensure that the messages communicated are regularly reviewed and updated.

It is therefore critical that people are suitably informed and prepared. The most effective way to communicate information to a mass audience is through an awareness raising campaign, and the effectiveness of that campaign largely depends on the strategy used.

About ENISA

The European Network and Information Security Agency (ENISA) is a European Union Agency created to advance the functioning of the Internal Market.

ENISA is a centre of excellence for the EU Member States and EU Institutions in network and information security, giving advice and recommendations and being a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the EU-institutions, the Members States and the private business & industry actors.

Contact Details:

For contacting ENISA or for general enquiries on Member States awareness programmes, please use the following details:

e-mail: Isabella Santa - awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Acknowledgements

Several parties supported and contributed directly or indirectly to this work in a number of ways. The information included in this Information Package, with few exceptions, includes contributions from Member States, bodies and organisations.

The authors wish to acknowledge the efforts of OECD, in particular of Mrs. Anne Carblanc and Mr. Laurent Bernat, whose initial support and co-operation have influenced some prevailing aspects of this project, the Member States and the PSG of ENISA, which provided valuable inputs and material for the compilation of the Information Package.

Additionally, the authors would like to thank the following organisations for the prompt support in the preparation of this document: CASPUR, City of Stockholm, Deloitte, FOURTH, Reuters, National Post and Telecom Agency of Sweden, SAP, SAFT, Swiss Re, University ‘La Sapienza’ of Rome, VigiTrust. Special thank to Mr. Jeremy Hilton for his research and valuable suggestions.

Finally, we would like to acknowledge the individuals who contributed to this document with informal reviews, valuable insights, observations, suggestions, and fixes. While this is undoubtedly not a complete list, this content would be incomplete and incorrect without their help.

Glossary

The following table details the technical terms with associated definitions used within this Information Package. For coverage of other terms and for more details, refer to the ENISA website: http://www.enisa.europa.eu/pages/05_03.htm

Term	**Definition**
A	
Adware	A program, often installed without the knowledge of a user through such actions as visiting websites or downloading software, which pushes and displays paid advertising
Anti-virus software	Software that is used to protect a computer against viruses or other malware threats. The software needs to be regularly updated and can also be used for security such as content or website filtering
B	
Botnet (Bots)	A network of compromised machines that can be remotely controlled by a hacker. Multiple bots joined together can be used to send spam or to launch Denial of Service attacks
C	
CERT	Computer Emergency Response Team - a coordination centre or group readily available to respond to and tackle any emergency computer and network security incidents
D	
Denial of Service	When a hacker floods an organisation's online business with false or fraudulent traffic with the intent of causing the website/portal to fall over
F	
Firewall	A device or software designed to stop unauthorised people accessing a computer via the Internet without permission
H	
Hacker	Someone who illegitimately gains access to, and potentially tampers with, information in a computer system
I	
Identity Theft (Fraud)	When personal details have been stolen and used illegally
Intrusion Detection System	Software that is designed to monitor and alert users on unauthorised access of a computer through the Internet
ISP	Internet Service Provider. Enterprise that provides an Internet service
M	
Malware	Malicious Software encompassing viruses, worms and Trojan horses amongst other bits of code
P	
Patch	An update to a program such as antivirus software or an operating system such as Windows. Patches can be obtained manually or automatically depending on user preferences
Pharming	A form of domain name spoofing that results in users believing they are on a genuine site with the correct URL only to be diverted to a scam site
Phishing	The practice of tricking a user into giving away personal information such as bank account details by pretending to be a legitimate business or organisation
S	
SMS	Short Message Service. Primarily used as a form of text based communication with mobile phones
Social Engineering	The practice of outsiders getting someone to do something that they might not otherwise have done
Spam	Unsolicited email that the recipient typically does not want to receive. The spam

Term	Definition
	can be either benign or a form of malware
Spyware	A program that monitors your Internet activity and transmits that information to someone else
T	
Trojan Horse	A program that appears to be useful but actually causes damage in some form. The goal of a Trojan Horse is to trick users by hiding the underlying activity
V	
Virus	A program that attaches itself to another program or data file in order to spread and reproduce itself without the knowledge of the user
W	
Worm	A program that reproduces by replicating itself across computer systems

Profile of Groups

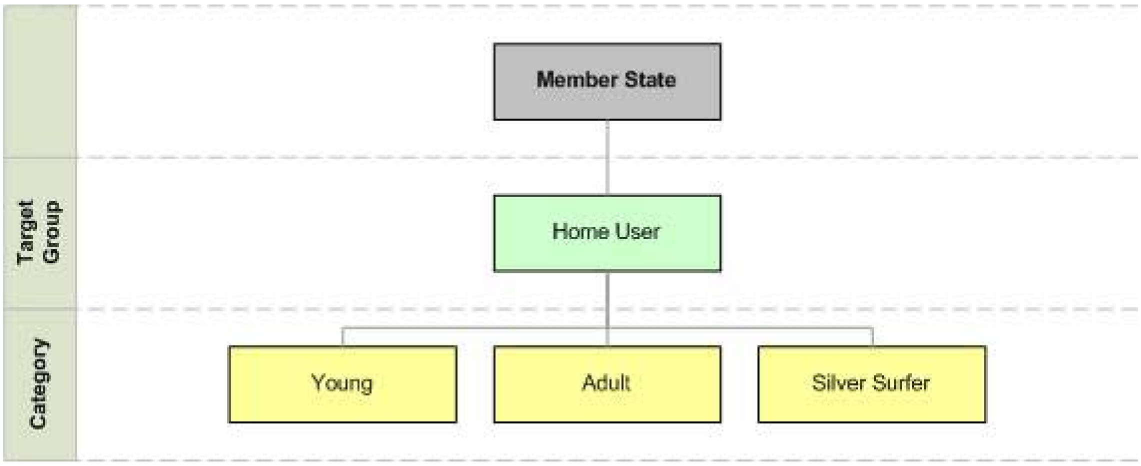
Before detailing the profiles of the five target groups focused on in this Information Package, it is worthwhile understanding some of the key terms used when describing these groups:

Term	Definition
Target Group	The specific audience that is targeted. This is either Home User, SME, Media, ISP or Local Government
Category	The classification or type of target group. For example, an “Adult” is a type of “Home User”
Sub Category	The classification or type of target group if the category can be broken down further. For example, an “Employee” is part of a “Small” business which is an “SME”
Interest/Need	The main activities the target group use ICTs to complete. An example would be for an adult to use the Internet for online banking
Knowledge	The technical aptitude level of the target group. This can be measured as “None”, “Low”, “Medium” or “High”
Channel	The form of communication (or media) used to deliver a message as part of an awareness raising initiative. An example would be a brochure

Understanding the terms used, it is possible to profile each of the five target groups:

Home User

Citizens with varying age and technical knowledge who use ICTs for personal use anywhere outside their work environments. This group of users can be further divided into three categories:



Young

Typically between 7 and 15 years old**,** these citizens have grown up in an ICT environment with their levels of knowledge largely dictated by the state of infrastructure in each of the Member States. These citizens are incredibly trustworthy due to their youth, have a high capacity for learning and are often of the mind to experiment with technologies.

Main Issues

- The young have no or at best a vague understanding of the range of information security threats existing. This makes them a weak link to be taken advantage of by hackers and fraudsters
- With no or little clear boundary on the Internet regarding such things as legal borders, the young need to be taught "what is right, what is wrong", similar to how they are taught about the real world
- The young are not learning from their parents when it comes to Internet safety
- The young typically are both trusting and inquisitive

Interests/Needs

- Playing games
- Online chat
- Surfing the web for interesting information
- Downloading music
- Mobiles
- Completing homework

Adult

Citizens born after the 1950s and older than 16 years of age**,** this group have partly grown up in an ICT environment. These users probably have the most diverse range of skills and knowledge of ICTs as compared to the other groups, ranging from nothing to a high level of sophistication. The citizens can be parents or childless, with any type of career.

Main Issues

- Though some adults have an adequate knowledge of some of the more common types of information security threats, they are not aware of relatively newer threats. For example, short range data exchange technologies such as Bluetooth are also affected by security and privacy issues. People are still unaware that someone can access their address book or make calls by connecting with their PDA or mobile phone through using Bluetooth

- Adults are failing to make financial transactions online (such as banking) due to a perception of a lack of security
- Adults are afraid of or do not understand all the terms and definitions used in campaigns and worry that they don't have time to understand a complicated message

Interests/Needs

- Online shopping
- Downloading music and software
- Payment online – shopping, phone bill, transaction activities etc
- Watching online entertainment
- Surfing informative websites – news, hobbies etc

Silver Surfer

Citizens born in the 1950s or earlier, having grown up in a non-ICT environment. Their level of knowledge is low to non-existent and though they are typically not technically oriented, they can be service oriented (for example using mobile based e-services). As the citizens have not grown up with ICTs, they may be more doubtful of or mistrust technology.

Main Issues

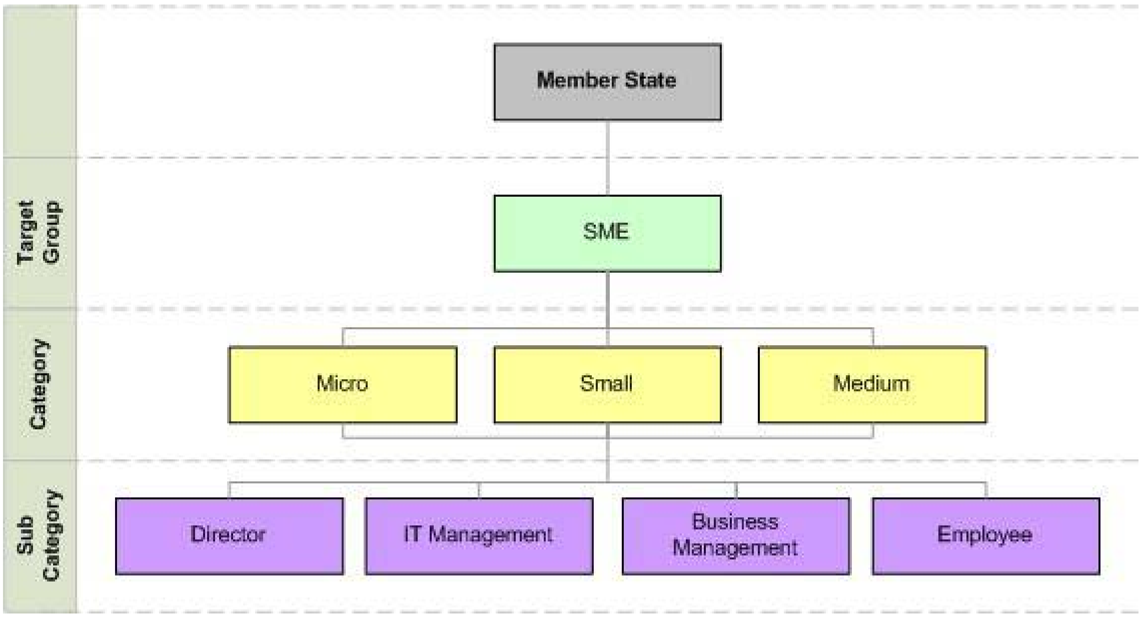
- Silver Surfers need to be informed of the economic risks, repercussions and the solutions to information security issues as they have not grown up with ICTs
- The average Silver Surfer has a “trusted” approach, though they are more fearful of security risks

Interests/Needs

- Access to online services or communications such as healthcare
- Communicating with family – staying in contact with loved ones via email etc

SME

Both employers and employees of micro, small or medium sized enterprises (businesses). The European Commission classifies medium enterprises as having less than 250 employees, small enterprises as having less than 50 employees and micro as those with less than 10 employees.[4] The size classification of the type of business does however vary across the individual Member States. This target group is extremely important constituting 99% of the total number of enterprises in the EU, encompassing some 65 million jobs. This group of users can be further divided into three categories each with four sub-categories:



Micro – a micro enterprise is defined as an enterprise that employs fewer than 10 people with an annual turnover and/or annual balance sheet of less than €2 million. Typically, this group of citizens does not have in-house IT or security experts. The numbers vary by Member State; for example in the UK a micro enterprise is typically comprised of fewer than five people.

Small – a small enterprise is defined as an enterprise that employs fewer than 50 people with an annual turnover and/or annual balance sheet total less than €10 million. The definition of a small business or enterprise also varies among Member States. A small business may or may not have an IT expert and is unlikely to have a security expert.

Medium – a medium-sized enterprise is defined as an enterprise that employs fewer than 250 people and which have an annual turnover not exceeding €50 million,

[4] Recommendation 2003/361/EC, OJ L 124 of 20.05.2003, p. 36. For more details on SME definition see http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/index_en.htm

and/or annual balance sheet total not exceeding €43 million. The definition of a medium business or enterprise varies among Member States. Typically, a medium sized business has an IT expert and may have someone with security knowledge.

Enterprise category	Headcount	Turnover	or	Balance sheet total
medium-sized	< 250	≤ € 50 million		≤ € 43 million
small	< 50	≤ € 10 million		≤ € 10 million
micro	< 10	≤ € 2 million		≤ € 2 million

Within each of the three target group categories, four sub-categories of user can be defined:

Director/Owner

The key decision maker for investment in security.

Main Issues

- Directors or owners of companies are often not realising the potential effects a serious information security breach can have to their business. Some examples of the types of threats to security a business is typically faced with include:
  - Virus infection and disruptive software
  - Staff misuse of information systems
  - System failures
  - Data corruption
  - Unauthorised access by outsiders, including competitors and hackers
  - Denial of service attacks
  - Disgruntled employees
  - Fraud, theft and deception[5]
- Information Security Management is not being seen as something that fits into the overall governance, risk management and compliance initiatives of a business, but rather as an extra financial cost and burden. It should be seen as something that can help prevent or minimise issues such as the disruption to operations, impacts to reputation or the effects on client and supplier confidence to the business
- A significant amount of businesses do not have Business Continuity Plans, or those that have do not regularly test them
- Information security is not being seen as a business enabler, but more as a business inhibitor

Interests/Needs

- Security framework that is robust and minimises disruptions to business
- Use of Internet and other ICTs to support business functions and activities
- Use of ICTs to support job interests including analysis tools, liability issues and organizational operations
- Day-to-day interests and needs are similar to those of Home User adults

IT Management

[5] DTI Information Security Breaches Survey 2004

Technically inclined, this group of users may not be security experts but need to understand and implement information security protocols.

Main Issues

- IT Managers or staff can get into the trap of helping to designing and implementing a security framework largely based on IT hardware and software, but can overlook two things: the need for a robust set of policies and procedures and the need for better human behaviour towards security
- This target group is generally technical in nature however specific messages may be overlooked as being perceived as non-technical or irrelevant or as too technical and aimed at larger organizations
- Businesses often do not have an information security framework, or if they do it isn't continually monitored or updated. Certain businesses do not have any type of Information Security Management System (ISMS)
- National and International standards such as ISO 17799 and other recognised standards such as COBIT are not being implemented, or if they are then certain controls such as awareness raising or assignment of roles and responsibilities are not being communicated effectively. Monitor and seek improvements controls are also not being implemented sufficiently6

Some of the target group needs to use an Information System Security Risk Management methodology of Prevention, Detection, Response and Recovery, but have inadequate controls in place to do so[7]

Interests/Needs

- Security framework that is robust and minimises disruptions to business
- Use of Internet and other ICTs to support business functions and activities
- Use of ICTs to support job interests including analysis tools, organizational operations and support manuals
- Day-to-day interests and needs are similar to those of Home User adults

Business Management

Often not technically orientated, this group of users need to be educated and understand the importance of information security. This will allow them to implement the relevant security policies and controls in their business areas.

[6] Achieving Best Practice in your Business - Information Security: BS 7799 and the Data Protection Act, DTI, 2004, http://www.dti.gov.uk/industries/information_security

[7] The Management of Security Risks in Information (paper), Philippe Bouvier, Thales Security Systems, 2004.

Main Issues

- Managers often fail to realise the implications of information security breaches. Apart from the hassle of an incident, other results (depending on the type and severity of the incident) can be[8]:
  - Loss of vital information and inability to function
  - Lack of professionalism in eyes of customer
  - Loss of confidential customer information
  - Loss of or compromise in trust and relationship with staff, customers and suppliers
  - Damage to Brand through appearing vulnerable
  - Cost of recovery, repair and management time
  - Cost of disciplinary action
  - Reduced efficiency
- Management sometimes do not actively support and implement the security policies and procedures within their own business areas
- In some cases, awareness to staff for their responsibilities as well as security issues in general are not being effectively communicated
- Information security protection is not seen as an ongoing set of activities but as something that can be implemented once
- Business Management can face similar issues as to those described in the previous text detailing *IT Management*

Interests/Needs

- Use of Internet and other ICTs to support business functions and activities as well as administration tasks
- Assurance that information using ICTs is confidential and private
- Day-to-day interests and needs are similar to those of Home User adults and other SME users

Employee

The largest number of users within the target group and arguably the most important if, as research suggests, most of the information security breaches are caused by human error.

Main Issues

- In the majority of cases, employees want to do the correct thing with respect to information security however they frequently don't know what that is

[8] Achieving Best Practice in your Business - Information Security: Hard Facts, DTI, 2004, http://www.dti.gov.uk/industries/information_security

- Users should be following clear and documented information security policies and supporting procedures however in a lot of cases they have no clear visibility
- There is a lack of adequate knowledge as to why security controls are needed and an employees responsibility to adopt them

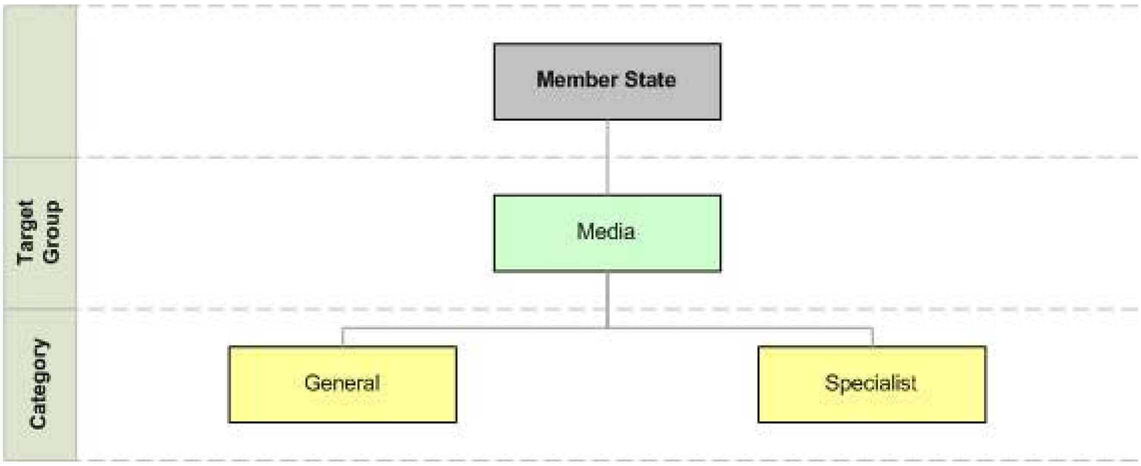
Interests/Needs

- Using ICTs to perform work related or administration tasks
- Assurance that any action online is confidential and private
- Day-to-day interests and needs are similar to those of Home User adults

For the purposes of this document, micro, small and medium enterprises will be considered as one entity (SME) as the three categories are often targeted as one in Member State countries.

Media

This target group is very important, primarily due to the influence they exert with the general public. If personnel within the Media world are themselves more aware of information security issues and corresponding solutions for not only their day-to-day work but also in general, then they can better inform their audience. Also, by making users in Media more aware, they themselves might put more emphasis on reporting the information. This group of users can be further divided into two categories:



General

Consists of journalists, writers, speakers and back room staff working in the mass media channels such as television, websites, radio and newspapers. Typically their target audience is the average citizen.

Main Issues

- Time, resource and effort that can be devoted to any one story is scarce
- There is an abundance of news regarding information and security so the coverage of stories dedicated to information security might be affected

Interests/Needs

- Report stories that are accurate
- Keep the public and fellow staff informed with topical and relevant up-to-date information
- Positively influence or better inform the public (dependent on the story)

Specialist

Consists of journalists, writers, speakers and back room staff working in specialised media channels focusing in a particular area. For example computer magazines or dedicated websites are forms of Specialist Media.

Main Issues

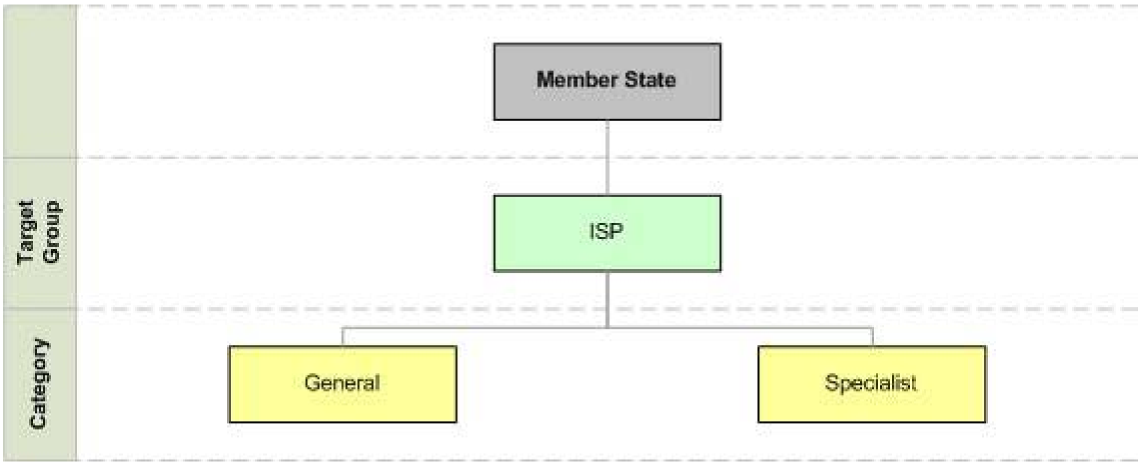
- The main issues facing Specialist Media are similar to those listed in the Media General section

Interests/Needs

- The Interests and needs are similar to those listed in the Media General section

ISP

This target group is important, primarily due to the fact that they are often the first line of defence and awareness for businesses and the general public when it comes to information security. This is because ISPs provide the service to access the Internet. If personnel within ISPs are themselves more aware of information security issues and corresponding solutions for not only their day-to-day work but also in general, then that can only help enforce the security to the general public. This group of users can be further divided into two categories:



General

Consists of private sector firms that offer a diverse range of products and services; areas covered are more than just offering an Internet sign-up and connection service. In addition to a subscription for online access, services may include email, chat, customised web portals, WiFi hotspots or media content such as video or music. The target audience for ISPs comprise of both businesses and citizens.

Main Issues

- State of technology and standards are continually changing
- Enforcement needs to be stronger as issues have downstream implications for anyone subscribing to the service offered
- Messages cannot be overly negative as could turn away business

Interests/Needs

- Keep the public and fellow staff informed with topical and relevant up-to-date information
- Positively influence the behaviour of the public, resulting in less issues to be solved
- Maintain and attract new business by reputation of security and services offered

Specialist

Similar to “General” ISPs – the only difference is that the range of products and services are either for a niche market or the depth of services is more restrictive. Typically, this group just offers a subscription for access to the Internet.

Main Issues

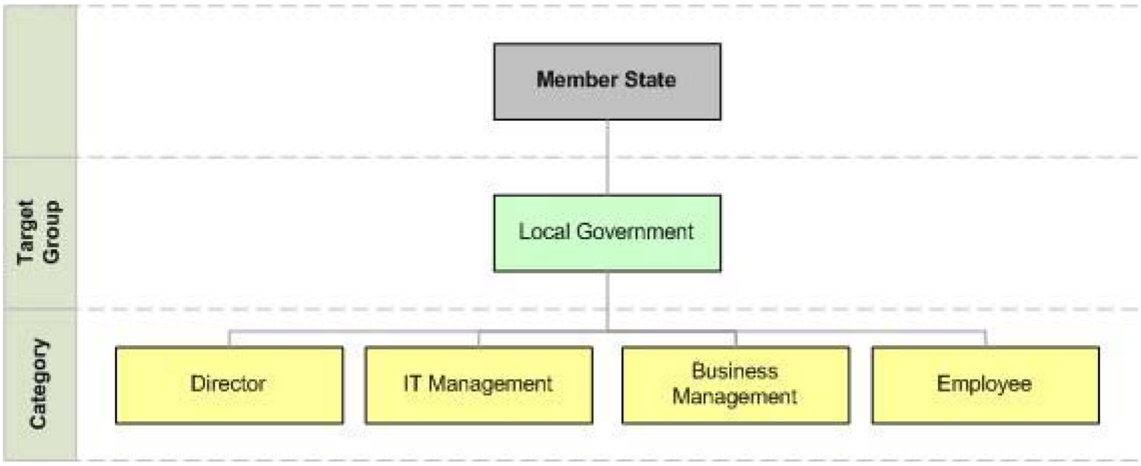
- The main issues facing Specialist ISPs are similar to those listed in the *ISP General* section

Interests/Needs

- The Interests and needs are similar to those listed in the *ISP General* section

Local Government

This target group is important in that it needs to be seen as being strong and secure when it comes to information security. Due to the nature of services offered, private and confidential information is often processed which has far reaching implications if breached. Different Member States have a different political setup, however all share the common goals of providing a safe and secure service to the public, whether it be from conventional contact such as through face-to-face services, through to modern e-Services utilising technologies such as online transaction technologies. The group of users that make up Local Government can be broken down in-line to the sub-categories used for the SME target group:



Director, IT Management, Business Management and Employee

For details behind each of the categories, refer to the relevant text in the *Profile of Groups* section for the SME target group.

Main Issues

- Refer to the main issues detailed in the previous sections for the SME target group
- In addition, Local Government users have to face public service compliancy procedures and protocols

Interests/Needs

- Refer to the interests and needs detailed in the previous sections for the SME target group
- In addition, Local Government users need to offer secure and efficient services within the workplace and also when communicating with the public

Good Practices Index

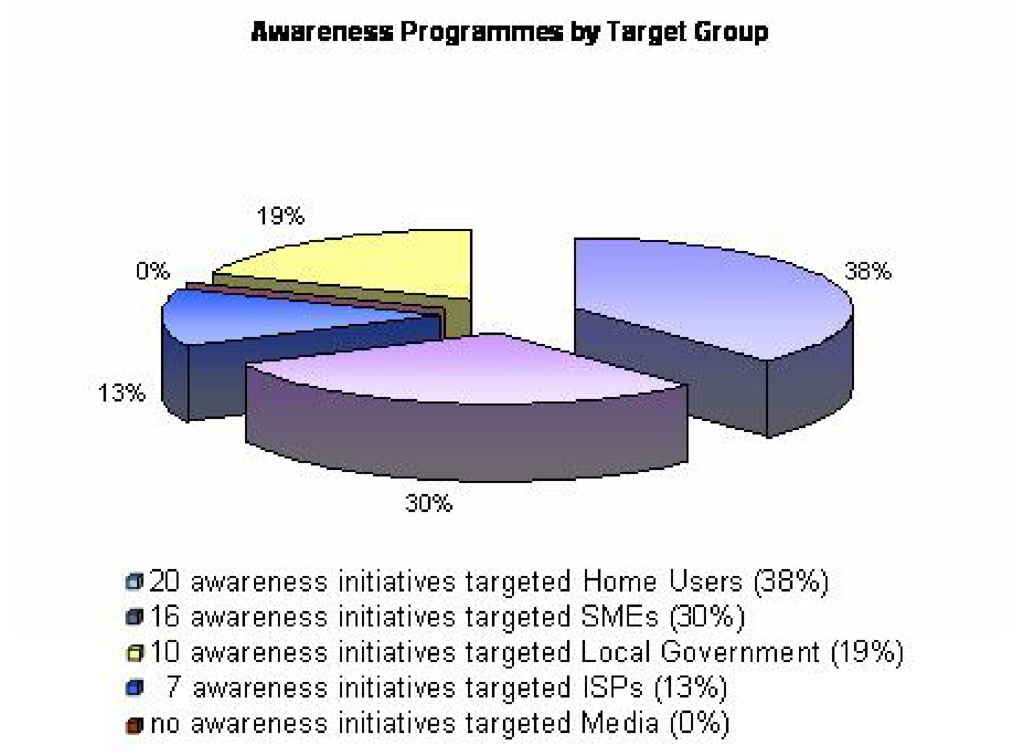
The following matrix acts as an index to the types of answers and detail of information provided by the Member State countries in responding to the questionnaire:

- The "Member States" column represents the name of the country that was sent the questionnaire to
- Member States (rows) have been grouped together using different colours. Countries have been grouped by similarities related to culture, knowledge, experience, interest/needs of target groups and language. Grouping is for indicative purposes only
- The columns in "Questions Answered" represent the shortened names of the different sections to the questionnaire. A "X" in a row indicates that the Member State provided information or an answer for that section
- The columns in "Target Group Info" represent the five target groups profiled in the Information Package. A "X" in a row indicates that the Member State provided information for that particular group
- The "Material Available" column indicates that ENISA has reviewed the material which has been developed within the Member States. An "X" in the row indicates that the material developed can be used as a basis for the development of material for a campaign in a different Member State or be entirely re-used. It should be noted that most of the material has been developed in the official language(s) of the Member States
- The "Referenced Websites" column represents the URLs provided by Member States when responding to the questionnaire

	Member States	Questions Answered						Target Group Info					Add. Info				Referenced Websites
		Gov. as developer	Nat. Gov. as user	Local Gov. as user	Gov. as partner (business)	Gov. as partner (society)	Metrics/KPIs	Home User	SME	Media	ISP	Local Gov.	Current Situation	Campaign Initiatives	Lessons Learnt	Material Available	
1.	Austria				X			X	X				X			X	http://www.it-safe.at, http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=209879&BrID=0&DstID=5344, http://www.it-safe.at/siha/fragebogen.html, http://www.ocg.at/publikationen/books/volumes/sr181.html, http://www.cio.gv.at/securenetworks/sihb/
2.	Belgium							X						X		X	http://www.click2win.be, http://www.web4me.be
3.	Cyprus	X												X			
4.	Czech Republic	X	X	X	X				X								http://www.micr.cz/nppg.html
5.	Denmark	X			X	X		X	X				X	X		X	www.it-borger.dk/netsikkernu, www.netsikkernu.dk
6.	Estonia	X	X	X	X	X	X										http://www.egov-goodpractice.org
7.	Finland				X	X		X	X					X		X	www.tietoturvaopas.fi, http://www.pelastakaalapset.fi/hiiripiiri/, http://www.pelastakaalapset.fi/nettivihje/english/
8.	France	X				X		X			X					X	http://www.famille.gouv.fr/protec_enfance
9.	Germany	X	X	X	X	X	X	X	X			X				X	www.bsi.bund.de, www.bsi-fuer-buerger.de, www.bsi.de/literat/buanzg.htm, www.bsi.de/literat/brosch.htm, www.bsi.de/literat/index.htm, http://www.bsi.bund.de/english/index.htm, www.bsi.de/english/gshb/guidelines/index.htm, www.bsi.de/gshb/deutsch/musterrichtlinien/index.htm, www.bsi.de/gshb/deutsch/hilfmi/beispielprofile.htm, www.teletrust.de, www.mcert.de, www.initiatived21.de
10.	Greece							X					X	X		X	http://www.saferInternet.gr
11.	Hungary	X	X	X	X	X	X	X	X			X	X			X	www.ihm.gov.hu, www.biztonsagosInternet.hu, www.halozatbiztonsag.hu, www.english.itktb.hu/Engine.aspx, www.meh.hu/szervezet/hivatalok/ekk/kietb/kietb20041116.html, www.nhh.hu, www.spam.baratsagosInternet.hu, www.magyarorszag.hu, www.telehaz.hu, www.itmentor.hu, www.esec.hu, www.iszt.hu/iszt/English, www.ivsz.hu, www.Internethotline.hu, www.matisz.hu, www.mte.hu, www.inforum.org.hu
12.	Iceland							X						X		X	www.saft.is
13.	Ireland				X		X		X			X		X			
14.	Italy	X	X	X		X		X	X		X	X		X		X	www.cnipa.gov.it/site/it-it/La_Documentazione/Pubblicazioni/i_Quaderni/, www.cnipa.gov.it/site/it-it/Attivit%c3%a0/Sicurezza_informatica/, http://www.cnipa.gov.it, http://www.italia.gov.it
15.	Latvia	X	X	X	X	X	X										
16.	Liechtenstein																
17.	Lithuania	X	X		X	X		X	X			X				X	www.esaugumas.lt, www.vrm.lt, www.securityconference.rrt.lt, http://www.esaugumas.lt/VRM/VRM/index.html
18.	Luxembourg	X	X	X	X	X	X	X	X		X	X			X	X	www.cases.lu, www.mysecureit.lu, www.petitweb.lu
19.	Malta	X	X	X	X	X	X	X	X		X					X	http://www.miti.gov.mt/site/page.aspx?pageid=4, www.miti.gov.mt

20.	**Netherlands**	X	X	X	X	X		X	X			X				X	www.digibewust.nl, www.ecp.nl, www.surfsafe.nl, http://www.onderzoeksdatabank.minez.nl/onderzoeken/onderzoekskaart.aspx?onderzoekID=2934, http://www.onderzoeksdatabank.minez.nl/rapporten/Rapport.aspx?rapportId=485, www.waarschuwingsdienst.nl
21.	**Norway**	X			X	X		X	X		X					X	www.norsis.no, www.nettvett.no
22.	**Poland**	X	X	X				X	X		X						www.zpp.pl, http://hotline.org.pl/, www.saferInternet.pl, www.dzieckowsieci.pl, http://www.cert.pl
23.	**Portugal**	X						X			X	X					www.umic.pt, www.cert.pt, www.ina.pt, www.crie.min-edu.pt, www.fccn.pt
24.	**Slovakia**	X	X	X	X	X	X										
25.	**Slovenia**	X	X	X	X	X	X	X					X				http://www.zrss.si/, http://www.safe.si, http://www.ris.org/index.php?fl=0&p1=276&p2=285&p3=&id=334
26.	**Spain**																
27.	**Sweden**	X	X	X	X	X	X	X	X			X	X	X	X	X	http://www.pts.se/Default.asp?Sectionid=&Itemid=&Languageid=EN, http://www.sitic.se/eng/index.html, http://www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646, http://www.konsumentverket.se/mallar/en/lista_artiklar.asp?lngCategoryId=922, http://www.verva.se/web/t/Page____492.aspx, http://www.krisberedskapsmyndigheten.se/6193.epibrw, http://kikaren.skl.se/artikel.asp?C=756&A=180, http://www.pts.se/Nyheter/pressmeddelande.asp?ItemId=4718, www.pts.se/internetsakerhet, www.testadatorn.se , http://www.surfalugnt.se
28.	**United Kingdom**	X	X	X	X	X	X	X	X			X	X	X		X	www.cctmark.gov.uk, www.itsafe.gov.uk, www.getsafeonline.org, www.cabinetoffice.gov.uk/csia/ia_governance/content.asp, http://www.niscc.gov.uk/niscc/warpInfo-en.html, www.dti.gov.uk/sectors/infosec, www.kable.co.uk, www.securityhealthcheck.dti.gov.uk, www.cbi.org.uk, www.bobs-business.co.uk, www.instisp.org, www.security-survey.gov.uk, http://www.wda.co.uk/index.cfm/technology_and_innovation/mtp/partner_programme/ecrime/en8118, http://www.internetsafetyzone.co.uk

Categorising the responses from the Member States, the following graph illustrates:



Good Practices by Country

The information captured in the following section correlates to the answers of the ENISA questionnaire that were received back from the Member States and/or to additional information and material provided by other bodies/organisations. It is worth noting that:

- For consistency, the structure of the questions are similar to those used by the OECD in creation of the 2005 “The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries” report
- Where a section does not exist, it is because no information was supplied by the Member States
- The “Current Situation”, “Campaign Initiatives” or the “Lessons Learnt” sections for each country have detail where Member States provided supplementary or alternate information to the answers of the questionnaire

1. Austria

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Austria have been detailed:

Current Situation

Government as partner with business and industry

Campaign Initiatives

Current Situation

- As in all other EU Member States, the importance of small and medium-sized enterprises for the Austrian economy is overwhelming. 99.8% of all enterprises are small or medium-sized (enterprises with up to 500 employees) with an average of about 10 employees per company
- Total number of enterprises, in particular of micro enterprises, has increased in the years 1988 to 1993. Since employment grew at a similar rate, the average size of enterprises has remained stable. However, business formation was considerably less dynamic in Austria than in other European countries such as Germany, Belgium, Denmark or the Netherlands
- All sectors of private economy in Austria, especially crafts, services and tourism are dominated by SMEs, although large enterprises contribute to the total employment in industrial manufacturing and transport
- Some 195,000 private enterprises employed about 2 million people in Austria in 1993. About 500 enterprises were large ones, while more than 194,500 were SMEs with more than 75 % of all those employed

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

The IT-SAFE initiative

The awareness raising initiative IT-SAFE addressed small companies which so far have not considered and included data security in their plans and internal policies. The goal of this initiative is to raise information security awareness providing practical advice for enterprises on how to achieve this goal taking into consideration the profile (e.g. needs of the enterprise) of this target group.

Basically there are two main concerns:

- Safeguarding the computers used by the SMEs from external threats
- Avoiding data loss due to insufficient backup and data maintenance procedures

Every SME is unique and therefore has its own specific demands on IT-security. Moreover, it should be taken into consideration that the available information security frameworks, such as CobIT, ISO 17799/27001 or Common Criteria, are in almost all cases not suitable for smaller companies due to their alignment towards the needs of large enterprises.

Thus, the IT-SAFE initiative provides an online-questionnaire which assesses both the IT-infrastructure of a specific company and its required level of protection of a particular enterprise in order to customise and provide an individual version of the IT-SAFE handbook to raise information security awareness. The information covered in the handbook features step-by-step advice for an IT administrator to help secure the company's IT-infrastructure.

The individual version of the IT-SAFE handbook is produced either in HTML or Adobe Acrobat format.

The Austrian Chamber of Commerce, in association with the Federal Ministry of Economics and Labour (BMWA) and the Institute for Economic Support (WiFi), offered special promotions to the participating companies. They were offering a 75% subsidy to IT-security consulting fees up to 6 hours of consulting service. In addition, a software package containing security-relevant applications, such as anti-virus and anti-spyware programs, was included. Companies as Ikarus, Nimbus Datentechnik, Symantec and Microsoft sponsored this initiatives. The software was provided free of charge.

Interest/need

The security initiative IT-SAFE addresses SMEs with up to 25 employees and offers specific advice to the personnel responsible for IT taking into consideration their knowledge, interest and needs. Typically IT-SAFE is aimed at businesses with a low knowledge of information security. The materials and channels used were:

- Print version handbook
  - No prior expertise required
  - Easy to understand but still comprehensive
  - Free of charge available online
- Online handbook & website
  - Individual handbook
  - Two versions available: one for CEOs and one for administrators
  - Website with questionnaire
- Security-check in the enterprise
  - Free of charge anti-virus and data-safety software
  - Individual consulting
  - Consulting fees for six consulting hours subsidized

Since IT-SAFE was initiated by the Austrian Chamber of Commerce, the initiative had a lot of visibility and was quite successful.

For the future, there is the intention to reach a broader audience. Thus the handbook will be revisited to accommodate the interest, needs and knowledge of this target group.

Information regarding this initiative is available on line since one year. Refer to the links below for more information:

- http://www.it-safe.at
- http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=209879&BrID=0&DstID=5344
- http://www.it-safe.at/siha/fragebogen.html - Online Questionnaire and Handbook

Austrian IT security handbook

The Austrian IT security handbook is a guide to help realise a comprehensive IT-baseline protection in enterprises and organisations. Unlike the German IT Baseline protection manual, it is not as comprehensive (about 400 pages compared to 3.000 pages of the IT Baseline protection manual). Its content focuses more on risk management, which is covered in one of two parts. The second part deals with IT-security measures.

Awareness-program (part of the handbook)

Only by understanding and permanently motivating staff members, is it possible to implement security policies and rules within an organisation successfully. To achieve this, a comprehensive and organisation-wide awareness program is required. The awareness-program should consist of the following parts:

- Information of all staff-members about the IT-security policy of the organisation
- The IT-security policy targets of the institution as well as their explanation
- The importance of IT-security for the institution
- Organisation and responsibilities in the area of IT-security
- The risk analysis strategy
- The security classification of data
- Chosen security measures (in particular those which are valid for the whole organisation)

Refer to http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB_V2_2_Teil1.pdf for more information.

Interest/need

The handbook is primarily focused on the following with a low to medium knowledge level:

- IT personnel responsible for IT-security in government and firms
- Interested private person

The handbook is being continuously improved and enhanced.

- http://www.ocg.at/publikationen/books/volumes/sr181.html
- http://www.cio.gv.at/securenetworks/sihb/

Campaign Initiatives

SaferInternet - Saferinternet.at focuses on parents (article)[9]

Summary

New brochures and handouts about safe use of internet and mobile phones are available. The material addresses the role of parents and caretakers.

Details

Saferinternet.at is currently focusing on parents as a main target group for improving safety in terms of internet and mobile phone use of minors in Austria.

According to the latest Eurobarometer report an increasingly high number of parents in Austria have set rules concerning the use of modern technology and communication tools (63%). Awareness of how to report illegal internet content improved significantly (63%) as well. Despite these encouraging results many parents still worry about online risks and seek support on how to deal with these issues in their families.

For this reason Saferinternet.at recently published the brochure “Kein Stress mit Web and SMS – Fakten und Tipps für Eltern und Erziehungsberechtigte zum Umgang mit Internet und Handy” together with Familienverband Österreich, the largest Austrian family organisation. This brochure contains facts and tips on internet and mobile safety for parents and educators and gives special emphasis to media education. It will be distributed to 70,000 families throughout the country.

Reacting to current hot topics in Austria, such as bullying and access to harmful video content through mobile phones, Saferinternet.at has also developed handouts on these issues.

All material (available in German) can be downloaded from the Saferinternet.at website http://www.Saferinternet.at.

In addition, the awareness node organizes a large number of events for parents and caretakers, ranging from information evenings to combined workshops for parents and their children.

[9] http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0606/at.htm, 12th June 2006.

2. Belgium

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Belgium have been detailed:

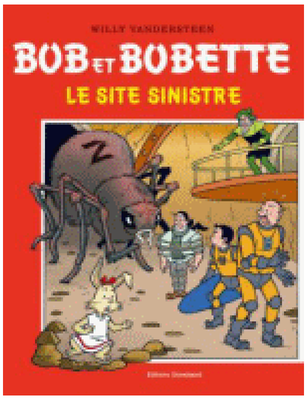
Campaign Initiatives

Campaign Initiatives

“Safe Use of the Internet” campaign

In Belgium, the “Safe Use of the Internet” campaign has been organised to promote awareness within children typically between 11-12 years. In order to effectively communicate the message of the campaign using the most appropriate communication channels, the organisers of the campaign have decided to produce a comic based on the popular series "Suske en Wiske" (in Dutch and German. In French, the title is “Bob et Bobette").

On 6th February 2006, Mr. Peter Van Velthoven (Minister for the Informatisation of the State), presented the comic in the three official languages: "De Sinistere Site" (in Dutch), "Le Site Sinistre" (in French) and "Der Listige Link" (in German).



The total number of albums printed was 120.000 (for the Dutch version), 80.000 (for the French version) and 1.500 (for the German version).

The comic, which is not available in bookshops, was distributed to the children of the sixth (and last) grade in all primary schools during the week of 27th March 2006.

It has been recognized that the channel used to help raise children awareness as part of the information security campaign was very effective as it had an instant appeal to the target group.

Moreover, as part of the campaign, at the age of 12 all Belgian citizens receive their national electronic ID-card with a free card-reader. This will enable them to chat safely online. The children will use defined websites. The goal is to reduce the chances for the children of making contact with people of ill intention.

To trap for informing better

The communication agency “Edge Communication” launched an information security awareness raising campaign. This new campaign lies within the scope of the European Safer Internet project and targets the youth between 14 and 18 years of age.

Through its website http://www.click2win.be , a fictitious mobile phone operator (CelBel) proposes offers such as free subscriptions for people up to 21 years old; this also includes SMS, Chat, MSN and email. To be registered, the web surfer must submit some personal data. Immediately after the subscription, a message appears on the screen explaining to the surfer that the new operator does not exist. The surfer is then invited to discover the “Web4me” website at http://www.web4me.be. Launched last May, the objective of the website is to promote the responsible use of the Internet by the youth.

The website also details associations and contact personnel that the youth should contact if faced with five types of threats:

- *Sectarian* - the opinion and information centre on harmful sectarian organisations, Centre d'information et d'avis sur les organisations sectaires nuisibles (CIAOSN)
- *Commercial* - the consumers information and research centre, Centre de recherche et d'information des organisations de consommateurs (CRIOC)
- *Technical* - the Internet Service Providers Association (ISPA)
- *Discriminatory* - the equal opportunity and fight against racism centre, Centre pour l'égalité des chances et la lutte contre le racisme
- *Pornographic* - the Child Focus association

The “CelBel” operator will maintain a presence on the web through banners and mailing lists. From the start of September, the fictitious operator will also be presented via peer-to-peer systems (systems like Kaaza that facilitate the exchange of computer files between private individuals.

3. Cyprus

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Cyprus have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

Campaign Initiatives

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

A policy paper on network and information security is currently being evaluated by the Minister of Communications and Works. It is expected that the Minister of Communications and Works will finalise the paper in September 2006, hence the implementation of the policy paper is estimated to commence by the end of the year.

As part of the policy paper on network and information security, measures regarding awareness raising are going to be implemented. Initially the Action Plan will be designed for raising awareness of end users, responsible public bodies for network and information security, other public and private bodies and businesses. The Action Plan is expected to be completed by the first quarter of 2007; hence its implementation is projected to commence in April 2007.

Legal, regulatory, and institutional arrangements to raise awareness

OCECPR is by Law (L.112(I)/2004) the responsible body for the co-ordination of networks and information security issues in Cyprus. OCECPR is the Cyprus representative in ENISA's Management Board and it acts as a central contact and coordination point between Cyprus and the European Agency.

Until recently there was no coordinated activity in this field in Cyprus. Certain actions have been taken for the protection of state and civil networks and services whereas private companies and organisations such as ISPs and Banks presented several initiatives. The great majority of companies in Cyprus, especially SMEs, are not showing particular interest in security issues mainly due to the high costs involved, their limited revenues due to the small size of their market, and the lack of obvious benefits (direct income) from such investments.

The framework for cooperation between public bodies and between public and private bodies will be set by the above mentioned policy paper as well as the prioritization of actions that will be taken in order to enhance network and information security policies. Awareness raising is one of the main issues of this policy paper.

Campaign Initiatives

OCECPR is currently undertaking a coordinative role in awareness raising and it plans to lead an initiative for the establishment of Work Groups that will see representatives of public institutions, banking institutions, academic institutions, developers and suppliers of network and information security systems, network and service providers of services and consumers protection organisations working together.

The effort will be aimed at educating and informing users, considering the characteristics of each target group, as well as in implementing concrete actions for the development of the appropriate security culture on security issues related with modern networks and exchange of information.

OCECPR is considering the experiences of other European countries which have had significant experience in this particular sector taking into consideration the diversity of the different parameters in each country, the social structure, the educational system, the enterprising system, the culture on using new electronic means and security measures, the structure of state economy and several other issues.

Successful examples will be considered if they can be adapted. These, in combination with several initiatives which will be undertaken in collaboration with other competent public as well as private institutions, will constitute the source for action for the best possible dissemination of appropriate information according to the needs of each user. Regarding business users of electronic communications networks and services, the effort will be targeted in the appropriate application of International standards on networks and information security, as well as in the establishment of suitable risk management policies on security issues.

4. Czech Republic

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Czech Republic have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

In order to provide an overview of the Czech national awareness raising strategy, a few organisations have been contacted. It appears that they don't have an *ad-hoc* strategy for raising awareness. Such initiatives are part of the activities of the Ministry competent for matters related to information systems.

The current work focuses mainly on tasks such as e-signature usage support, as well as on support for usage of qualified certificates in communication with public administration information systems (PAIS).

Legal, regulatory, and institutional arrangements to raise awareness

The main legislation is Act 227/2000 (regarding e-signature). The goal is to increase the support of e-signature usage as it is seen as being an important component of security.

Another piece of legislation, Act 365/2000 (regarding PAIS), has a new amendment which will govern the security and awareness raising in PAIS.

With regards to promotion of security as an essential component in public and private governance, the Ministry has collaborated with Microsoft. Practices from ENISA and other EU bodies have also been looked at.

National courses on information literacy (including security) exist. They target citizens.

For details on general issues, refer to http://www.micr.cz/nppg.html

National government as user of information systems

Recent awareness programmes and initiatives

One of the technical projects underway at the moment is for the creation of two meta-information PAIS. One of the goals of the implementation is to get users to accept actions; when they handle the data from the systems, the data must be e-signed.

Local government as user of information systems

Recent awareness programmes and initiatives

The following links can be used to gather information on the National program of information literacy. The site is in Czech:

- http://www.micr.cz/scripts/detail.php?id=3361
- http://www.micr.cz/scripts/detail.php?id=1930
- http://www.micr.cz/scripts/detail.php?id=2137
- http://www.micr.cz/scripts/detail.php?id=2813

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

The Ministry has worked with Microsoft on initiatives in an effort to promote information security. Currently no other private sector firm has been engaged. The Ministry has used the collaboration with Microsoft and practices from ENISA and other EU bodies for input into awareness raising activities.

5. Denmark

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Denmark have been detailed:

Current Situation

Government as developer of legal, regulatory and institutional arrangements to raise awareness

Government as partner with business and industry

Government as partner with civil society

Campaign Initiatives

Current Situation

- There is a need for information on IT security as more and more Danes are using the Internet on a daily basis. 79% has Internet access at home and 57% use the Internet every day. The main purposes are communication, information seeking and online services. The Ministry of Science, Technology and Innovation sees this as a positive development and wants to encourage the Danes to using the Internet, but also to think about how they use it
- The most current IT security problems in Denmark are spam mails, loss of information or time in response to computer virus. 35% of the Danish population have lost information in connection with virus attacks during 2005. 55% of the Danish population have lost data in connection with spam

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

Net-safe now! (annual event)

The Ministry of Science, Technology and Innovation has launched the public information campaign on IT security “Net-safe now!” for the second time. The Ministry has been cooperating with several different private and public institutions (among others Microsoft, Nordea, PBS etc.) on creating and carrying out the campaign.

The basis for the campaign

The Ministry of Science, Technology and Innovation and the campaign net-safe now! are aiming for creating awareness about IT security and a safe behaviour on the Internet. The campaign contains a number of activities in all Denmark.

The campaign comprises a series of activities focused on the target audience, e.g. teaching children and the elderly how to behave on the Internet. The campaign started off on 2nd May followed by activities during the month of May. The goal is to provide the target group with simple and easy-to-follow advice in order to improve the general knowledge and awareness of IT security.

In overall terms the main goal of the campaign is to spread the knowledge of IT security and to make the public aware of security issues arising from use of the Internet. The long-term objective is to contribute to the development of an IT security culture in Denmark by encouraging all IT users to act responsibly and thus operate more securely on the Internet.

Apart from the various campaign initiatives around the country, the campaign has been promoted in the media, such as national and local newspapers, on TV, radio and online. The campaign also includes a number of online activities that can be found via the campaign website www.it-borger.dk/netsikkernu. The website provides the users with all relevant information about the campaign such as the campaign calendar, a list of organizers and participants, and relevant links. Furthermore, they will find user-oriented information on IT.

Different channels of communications have been used to help raise awareness as part of this information security initiative.

The target groups

The selection of the target groups was decided in view of an analysis of the knowledge about IT security in the public. The report describes how the public can be split into two groups: one small group containing persons with strong knowledge on IT security and one big group containing people with less knowledge on IT security:

- Women
- Elderly people (+60)
- People who don't work with IT on a daily basis

The target audiences were including children (10-16 years), elderly people (+ 60 years), women and employees.

Cooperating partners

This campaign has been made possible by a substantial number of participants who contribute to the campaign in many different ways. Participants in the campaign are entitled to use the campaign logo (we support net-safe now!), developed to give the campaign a common recognisable brand. When using the campaign logo on the company website the different participants commit themselves to a Code of Conduct with simple guidelines.

The cooperating partners have attended in the different groups with different tasks. Ordinarily the cooperating firms are represented in all three groups with three different persons:

- Working group: The participants are most often IT employees with a special knowledge about what is important to inform about. The task of the group is to arrange activities, materials or events to take place on the campaign day. All the activities have to be in the framework of net-safe now! The participants in this group fill out a schedule describing considerations on media strategy, use of resources and logistics. By signing this schedule the participants commit themselves to carrying out the activity
- Media group: The participants in this group are most often PR or communication employees. The main task of the group is to see to it that the campaign is exposed in the media. The media group is responsible for contacting the press, finding angles to press releases, articles etc. This group had their first meeting a month earlier than the two other groups. The purpose of this meeting was to specify in more detail the target groups and how to reach them
- Steering group: The participants are most often representing the management of the firms. The main task of the group is to approve the overall message, the communication and media strategies, as well as the PR initiatives. Refer below for a list of all the participants

The webpage related to the campaign is www.netsikkernu.dk

Evaluation

The campaign consisted of 333 events, with 142 visits on Danish schools and 126 teaching courses in data processing centres for the elderly.

Related to the campaign the newspaper ”netsikker nu @visen” was produced in 120.000 copies. The newspaper contained several articles aimed at the different target groups. A film spot was also made (“Is Klaus at home?”), providing information about IT security in an easily accessible way. The film spot was a Danish version of the German “Wo ist Klaus?”. The newspaper was distributed through the cooperating partners and through the libraries, TDC stores and Nordea branches.

The film spot was also distributed through the cooperating partners and through a great amount of webpages. The film spot was shown 100.568 times.

The newspaper as well as the film spot was also available as downloads on the campaign webpage.

A series of materials were also produced:

- TV-spot about bullying on the Internet featuring a famous woman (Andrea Vagn Jensen) known from children programs among other things. The TV-spot was on three times a day on two different channels in the period 10th - 23rd April
- Rubber band with the print www.netsikkernu.dk
- Film made by children as the result of the project ”Safer internet day” that took place in February

Complete list of cooperating partners

Bornholms Erhvervsskole, Cyberhuset, DANSK IT, Dansk Metal, EA Vest, EUC Midt, EUC Nord, EUC Syd, Habbo Hotel, IT- og Telestyrelsen, ITB, ITEK/DI, Medierådet for børn og unge, Microsoft Danmark, Morgendagens heltinder, Niels Brock, Nordea, Odense tekniske skole, Parkegaard & Kristensen, PBS, Protego/PWC, Roskilde handelsskole, Syddansk universitet, TDC, TEC Ballerup, Uni-C, Vejle bibliotek, Vejle tekniske skole, Videnskabsministeriet, Vi Kvinder, Ældremobiliseringen.

Government as partner with business and industry

Recent awareness programmes and initiatives

Refer to the *Gov. as Developer* section for information on Net-safe now! campaign.

Government as partner with civil society

Recent awareness programmes and initiatives

Refer to *the Gov. as Developer* section for information on Net-safe now! campaign.

Campaign Initiatives

SaferInternet - Danish network knowledge (article)[10]

Summary

Procedures in relation to internet safety, knowledge about children's use of mobiles and the internet are some of the subjects on the agenda of the Danish awareness node's national network of stakeholders. Today the network counts 22 members.

Details

From the early rising of the Insafe network on internet safety awareness, the Danish awareness node (the Media Council) has been functioning as a national locus of knowledge on children and young people's use of the internet and new technologies. It has maintained a dialogue with Danish industry, public authorities, universities and organisations through a national stakeholder's group.

Through regular meetings and updates, the aim has been to create a network for the exchange of ideas, knowledge, best practise and procedures. The national newsletter for instance, keeps stakeholders up-to-date with news and information about children's and youth's media use. The newsletter is based on information received from national stakeholders and contains a direct link to the Insafe one.

The end result has been a number of awareness raising initiatives and projects made in cooperation between the various stakeholders. "The Youth Ring", an association of approximately 1,200 after school centres and youth clubs for 10 to 18 year-olds has been a member of the network since 2004. Flemming Moestrup, consultant in the association, emphasises how "the Youth Ring" has benefited from participating in the stakeholder group: “Receiving information and educational material as well as getting to know partners in our area has meant a lot to us, and has been very useful for our members”, says Flemming Moestrup.

He spells out the concrete results of the network with the example of "the Youth Ring": “We have earmarked resources to communicate the Media Council's research and recommendations on children's and young people's use of computer games, and internet behaviour. At the moment, this is the most sought after service in the Secretariat. We also

[10] http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0706/dk.htm, 3rd August 2006.

work in closer cooperation with a number of partners of the group – a possibility the stakeholder group has been the catalyst for.”

6. Estonia

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Estonia have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as partner with civil society

Metrics and key performance indicators (KPIs)

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The Estonian Ministry of Economic Affairs and Communications has prepared a nation-wide information security policy that specifies e-security related initiatives and coordinates them between the Estonian governmental organisations. The Estonian information security policy is under harmonization within the responsive ministries. The policy requires applying of the information security strategy, which is under development.

The main goal of the Estonian information security policy is a secure, security-aware, and enabling Estonian information society. Specific goals include elimination of non-acceptable risks, defence of basic human rights, information security awareness and training, as well as competitiveness of the economy.

The policy comprises five domains. The Estonian Ministry of Economic Affairs and Communications (MEAC) is coordinating the domain of e-security cooperation and coordination. The domain covers initiatives such as coordination of the Estonian ICT environment risk analysis, establishment and maintenance of the Estonian CERT (Computer Emergency Response Team), participation in the activities of ENISA (the European Network and Information Security Agency) and coordination of the cross-border initiatives.

The crisis management and cybercrime domain is served by the Ministry of Internal Affairs together with the Ministry of Defence. The domain includes preparation of the state crisis management plan, coordination of the work of the state and local crisis committees, as well as coordination of the international cybercrime related initiatives.

Secure e-Government must be based on appropriate legislation, standards, and procedures, such as security requirements for databases, services, and state procurement. The domain of regulations is coordinated by the MEAC together with the Ministry of Internal Affairs.

Both people and assets must be protected while using the e-Government applications. Coordination of e-security related tasks within applications, such distributing the ID card solutions and using the TESTA (Trans European Services for Telematics between Administrations) network, is performed in the application domain. The domain is assigned to the Ministry of Internal Affairs together with the Ministry of Defence.

To implement the information security policy, development and adoption of the annual action plan for the Estonian information and security policies is each year coordinated by the MEAC.

Further information is available as below:

- Press release by the Estonian Ministry of Economic Affairs and Communications
- Principles of the Estonian Information Policy 2004–2006
- IT in Public Administration of Estonia 2005

Legal, regulatory, and institutional arrangements to raise awareness

According to the information security policy, the Ministry of Education and Research, the Ministry of Defence, the Ministry of Economic Affairs and Communications, and the State Chancellery are responsible for the domain of education and training. The initiatives foreseen include PR activities, training, awareness websites, cooperation with the (high) schools, and satisfaction research.

The Personal Data Protection Act was accepted by Parliament on 12th June 1996. The act serves to protect the fundamental rights and freedoms of persons with respect to the processing of personal data and in accordance with the right of individuals to obtain freely any information which is disseminated for public use.

The protection of personal data is ensured by virtue of the fact that chief processors and authorised processors may process personal data only for purposes and under conditions which are specified in the Personal Data Protection Act. Individuals have the right to consent to the processing of personal data about them, to receive information concerning the processing, and to refuse permission to process personal data about them.

The Personal Data Protection Act divides personal data into two groups: non-sensitive and sensitive personal data. Sensitive personal data are data which reveal political opinions, religious or philosophical beliefs, ethnic or racial origin, the state of one's health, one's sexual life, criminal convictions, legal punishments and involvement in criminal proceedings.

Processing of non-sensitive personal data is permitted without the consent of the respective individual if it occurs under the terms which are set out in the Personal Data Protection Act. Sensitive personal data may be processed only with the consent of the respective person, unless the act provides otherwise.

Processed personal data are protected by organisational and technical measures which must be documented. Chief processors must register the processing of sensitive personal data with the data protection supervision authority, which is the Data Protection Department of the

Ministry of Internal Affairs. The Legal Committee of Parliament exercises supervision over the Data Protection Supervision Authority.

The other IT legislation includes among others the following acts:

- Digital Signatures Act
- Databases Act
- Archives Act
- State Secrets Act
- Official Statistics Act
- Public Procurement Act
- Electronic Communications Act
- Public Information Act
- Consumer Protection Act
- Legislating Digital Signatures in Estonia
- Principles of Estonian Information Policy

Estonia has been the chair country for the Northern eDimension eSecurity Action Line, which comprises the following main areas: investigation and exchange of good practices in the network and information infrastructure security area; digital signature interoperability; secure exchange of data between national population registers.

A number of eSecurity related seminars, presentations, articles and project proposals have been elaborated: the eGovernment cases "A Population-Wide ID card (Estonia)" and the "Special citizens web portal with Standard DB-services" are available on the *eGovernment Good Practice Framework* database (http://www.egov-goodpractice.org).

National government as user of information systems

Recent awareness programmes and initiatives

Both people and assets must be protected while using the e-Government applications. Coordination of e-security related tasks within applications, such distributing the ID card solutions and using the TESTA (Trans European Services for Telematics between Administrations) network, is performed in the application domain. The domain is assigned to the Ministry of Internal Affairs together with the Ministry of Defence.

Local government as user of information systems

Recent awareness programmes and initiatives

There has not been a separate security awareness raising program for users of local government systems.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

Important contributions to the development of information security awareness are standards and publications related to information security. These publications are available in Estonian. Some examples include:

- ISO/IEC 17799:2003 Information technology — Code of practice for information security management
- EVS-ISO/IEC TR 13335:1999 Information technology — Guidelines for the management of IT security (1-5)
- Governance, Control and Audit for Information and Related Technology (COBIT). Third Edition. Information Systems Audit and Control Foundation, Rolling Meadows, USA
- ISO TR 13569 Banking and related financial services - information security guidelines
- ISO/IEC 90003, Software engineering — Guidelines for the application of ISO 9001:2000 to computer software
- EVS-ISO/IEC 12207:1998 Information technology - Software life cycle processes
- ISO/IEC TR 15271:1998 Guide for ISO/IEC 12207 (Software life cycle processes)

Moreover, it has been planned to publish a special IT security web page which will focus on the security awareness raising issues including the ones related to SMEs.

Internet Service Providers (ISPs)

There has not been a separate security awareness raising program for different ISP customers in Estonia. There are plans to launch some campaigns and some special activities for raising security awareness level among internet users.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

There has not been a separate security awareness raising campaign with Media to promote a culture of security. The newspapers and journals often publish different security culture promoting articles. Most are written based on specific e-services or products e.g. how to use ID cards, how to securely use ecommerce services, how to protect the home users PCs, how to protect users in WiFi networks etc.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The “Look at world” project has been run some years ago. One of the goal of the project was to raise the computer awareness and skills levels of end users, trying to promote the use of e-services within the end users.

Future public-private partnerships

It has been explored the possibility to establish public-private partnerships in the future. At the moment, no concrete activities have been put in place.

Government as partner with civil society

Recent awareness programmes and initiatives

Estonia has participated to the Safer Internet Day blogathon on 7th February 2006.

There are also plans to publish a special IT security web portal which will focus on the security awareness raising issues among the home users.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The “Look at world” project has been run some years ago. One of the goals of the project was to raise the computer awareness and skills levels of end users, trying to promote the use of e-services within the end users.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

No KPIs for measuring security awareness initiatives have been developed or implemented.

Importance of Metrics/KPIs

It has been recognised the importance of metrics as they could help to compare the security awareness which has been raised with the success of different campaigns. It is difficult to suggest a concrete strategic approach for measuring the success of campaigns. It really depends on the campaign, how the campaign is organized and to whom it is focused.

7. Finland

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Finland have been detailed:

Government as partner with business and industry

Government as partner with civil society

Campaign Initiatives

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

The National Information Security Day 2006 Project provides information about safer internet use for the SMEs as defined within the ENISA's Information Package 2005. The main goal of the project is to provide a comprehensive picture of what is information security for the SMEs. The following areas have been taken into consideration: definition of information security, risk analysis, information security plan for an SME, safe use of ICT in every day business life.

The project, launched in February 2006, is an online service (www.tietoturvaopas.fi) for SMEs. The online service functions as a guide and it is especially targeted to those SMEs which do not yet have an operating and comprehensive information security practice in use. The web site includes many practical tools for both employers and employees in SMEs.

The National Information Security Day 2006 is one of the primary projects of the governmental Information Security Committee. The project is arranged by the public administration, business parties and various interested associations and organisations.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The National Information Security Day project is a versatile communication project to enhance knowledge of information security. The project is a co-operational project where about 30 organisations are involved. Public administration, business parties and various interested associations and organisations have been represented. The National Information Security Day 2005 is one of the primary projects of the governmental Information Security Committee. Target groups for this awareness raising project are school children, SMEs and internet home users.

The following organisations have been involved in this public-private partnership: Aina Group, Central Chamber of Commerce Finland, Federation of Finnish Enterprises, D-Fence, Elisa, Finnet Union, Finnish Macintosh User Group FiMUG, F-Secure, Hewlett-Packard, Association of Regional and Local Authorities, Consumer Agency, Ministry of Finance, Ministry of Education, Ministry of Trade and Industry, Ministry of Transport and Communications, the Mannerheim League for Child Welfare, Microsoft, National Emergency Supply Agency, National Board of Education, Panda Software Finland, Population Register Centre, Save the Children, TeliaSonera Finland, TIEKE Finnish Information Society Development Centre, Finnish Federation for Communications and Teleinformatics FiCom, Office of the Data Protection Ombudsman, Finnish Information Security Association, Information Society Programme, Finnish Communications Regulatory Authority, VTT Technical Research Centre of Finland

The Project is funded by the ministries and business parties listed above. Various interested organisations bring their expertise to the project. All the organisations are represented in the work groups which produce information and materials for the online services and plan and carry out a media campaign.

During the past three years, this public-private partnership has proved to work well. This kind of multi-organisation collaboration allows the project to have a versatile approach on the theme and to be heard broadly within the target groups.

Government as partner with civil society

Recent awareness programmes and initiatives

The National Information Security Day Project is a versatile communication project to enhance knowledge of information security. The project is a co-operational project where about 30 organisations are involved. Public administration, business parties and various interested associations and organisations have representation. The National Information Security Day 2005 is one of the primary projects of the governmental Information Security Committee. Target groups for this awareness raising project are school children, SMEs and the home users of the internet.

Home users have been a target group in the project for the past three years. During this time several activities have been carried out. In 2004 a Guide for the safer Internet at home (Joka Kodin Tietoturvaopas) was delivered to more than one million homes in Finland, and a web site (www.tietoturvaopas.fi) was launched. Since then the web site has been updated regularly.

The main issues covered on the web site are: how to protect your computer from malicious program and spam, how to use the online services safely, how to protect your privacy in the Internet, how to use different online connection safely, description of threats in the Internet and how to protect against them.

The topic of safer internet use has been discussed nation-wide i.e. on Information Security Day which is organized by The National Information Security Day Project. Home users are also reached throughout updates, press releases, advertisement on television, newspapers, magazines and Internet.

Campaign Initiatives

SaferInternet - Good practice in Finnish (article)[11]

Summary

In Finland good internet safety awareness practices include the Hiiripiiri handbook, the Safer Internet Day, the comic books for children and the collaboration with content providers.

Details

Hiiripiiri media safety literacy book:

4,000 Finnish school children received the Hiiripiiri internet and media safety literacy book in 2006. Hiiripiiri aims at building up a broad network involving learners, teachers, experts and stakeholders. Children should collect "Mousepoints" in order to receive a "Mouse Doctor" grade and certificate. Children's work on Hiiripiiri, tips on the tasks and new material produced by day-care centres and schools will be made available on the Hiiripiiri site: http://www.pelastakaalapset.fi/hiiripiiri/

Finnish Safer Internet Day targets schools:

The Finnish Safer Internet Day is part of a political program of the Finnish Government joining together almost all ministries, industrial co-operative unions, NGO's and, this year, also the Finnish trade and bank organisations. The costs of this initiative will be split between the biggest ISPs and software producers, and the government. This annual event will always target schools and children.

Comic books and stories for children and young:

The www.tietoturvakoulu.fi website supporting safer internet guidance has been broadened and updated based upon users' feedback. Two new comic book-type stories have been added emphasising three basic elements of safer internet use: follow rules, protect yourself and safeguard your computer:

- *Anne's New Friends* addresses young schoolchildren and concerns the public nature of the internet, the importance of privacy, photo publishing and copyright.

[11] http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0706/fi.htm, 31st July 2006.

- *Knots and Mishaps* is a story intended for children and looks at the true value of information on the internet, copyright issues, responsibility, and text and photo publishing.

The stories can be read individually, in groups or together with teachers. They contain information about safety and on line competitions to test the level of knowledge of information safety. Over 15,000 pupils have participated to the competition so far and 80% of school teachers have visited the web site.

Collaboration with content providers - go where the children are!:

The Children's voice questionnaire is published every May for the last 4 years. Collaboration with content providers has given the Finnish node free internet space on their sites and support for its aims and work. The questionnaires can be consulted at: http://www.pelastakaalapset.fi/nettivihje/english/

8. France

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for France have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

Government as partner with civil society

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

Refer to the *Gov. as Partner (Society)* section for information on awareness raising campaigns targeted at the young and parents.

Government as partner with civil society

Recent awareness programmes and initiatives

French Ministry of Family campaign (F@mille en ligne: "Sur internet, la securite ca commence aussi par vous")

Working Group on the Conference of the Family

Following the request of the Minister in charge of the Family, a working group has been created to prepare the Conference of the Family 2005. This working group brought together, once a week during three months, all the actors involved in the child protection on the Internet: ministries (Family, Interior, Justice, Industry, Education, Youth and Sports), family associations (association du movement familial), association of child welfare (association de protection de l'enfance), unions and web professionals (access providers, content editors, software editors, mobile phone operators, etc.). Experts were also involved including doctors, child psychiatrists, academics, specialised journalists and representatives of the French broadcasting authority (Conseil supérieur de l'audiovisuel), the French data protection authority (the Commission nationale informatique et libertés) and the Forum of the rights on the Internet (Forum des droits sur l'internet).

The working group was chaired by Joël THORAVAL, president of the National commission of human rights (Commission Nationale Consultative des Droits de l'Homme).

The objectives of the group were:

- To identify the way the children are using internet and their led behaviour, as well as the knowledge by the parents of these usages
- To establish families needs and expectations on the subject
- To define tools and necessary conditions for a secure practice of the Internet by the children

The group handed its report, "Protection de l'enfant et usages de l'Internet" (child protection and Internet use), to the Minister in charge of the Family, Philippe BAS.

Further to this preliminary document of dialogue and propositions, the Prime Minister announced during the Conference of the Family, which has been held last 22nd September 2005, three measures aimed at securing children in their usage of the Internet:

- The systematic proposal to the parents of an effective, free and upgradeable parental access control software

- The creation of a “label family” which will be a simple mark allowing parents to distinguish contents respectful of the protection of the child
- A general public awareness campaign, based on the broadcast of short films showing a family in its usage of the Internet

Family of Line awareness campaign

The Minister in charge of family also launched a general public communication campaign. The objective of the campaign was to inform the parents of the potential risks to which the minors are exposed with the web and to familiarize them with responsible use of the Internet. The Ministry broadcasted, as part of the "f@mille en ligne" program, a series of ten films. The films show the Internet experiments of a family and how they are informed about the various existing security solutions. Each 45 second episode was broadcasted twice on the two most favourite channels for children and youths in France (TF1 and M6) between 15th May 15th and 2nd June 2006.

This national information security awareness campaign intended to develop a constructive and positive dialogue within the family around Internet, with a double objective:

- to inform the parents of the potential risks of the internet for their children
- to familiarize families with responsible use of the Internet

The message consisted of indicating that "the public authority and the ISPs are mobilising themselves to propose free software of parental access control and protection of the family".

The key message of the campaign was “On the internet, security starts with you”.

Preliminary studies

The Ifop poll institute has been asked to carry out a survey to compare the parent’s knowledge and conscience of the use of internet made by their children to what the teenagers declare to do on the net.

The survey has been developed in two parts: "parents and the Internet use of their children" and “internet usage by the teenagers". This study highlighted in particular that:

- When 25 % of the teenagers declare to carry out purchases on the Internet, 91 % of the questioned parents affirm that their children never buy on the Net
- 42 % of the teenagers having a blog "never" or "rarely" speak about it with their parents
- 38 % of the teenagers “never” or “rarely” speak with their parents about their activities on the Net. And 69 % of them estimate that this "does not interest their parents"

- For 55 % of the teenagers knowing that the home computer is equipped with a parental control access software, 20% estimate that the software is "effective but easily avoidable", and 6 % consider the software "ineffective"
- 36 % of the teenagers declare that they have already been confronted more than once to "shocking, violent or pornographic images or contents, on the Net"
- Only 48 % of them spoke about it with their parents
- In parallel, a study of the delegation of the family indicated that in February 2006 only 15 % of home internet connections were equipped with parental access control software
- Finally, at the end of 2004, a CREDOC study stated that when 75 % of the 11-17 years said they were "familiarized" with the technological environment of the Internet, only 45 % of the parents were in the same case

Campaign target

Target groups for the "F@mille in line” campaign were: the general public, the parents of children and teenagers surfing the web, the teenagers of the age of 11 - 17 years old.

Concept

On the principle of a subjective camera (the spectator is "in" the computer screen), the members of a family using the Internet can be seen. Through their experiments, various topics are approached:

- personal and banking data protection
- blocking of undesirable websites and mail
- monitoring of the dependence to the play, etc.

The campaign encourages parents to keep control.

Channels used

- Television at audience pics (TF1, M6); 45 second films broadcasted just before the news. Refer to end of this section for information about each of the short films
- Websites of the ministries involved: Prime Minister, Family, Industry, National Education, Interior, Justice, Youth and Sports; banners with campaign logo linked to the Ministry for the family website
- Web portals of the private partners (16th November agreement signatories ISP): banners with campaign logo linked to their own informational page on the campaign

Multipliers

Last April, the ISPs launched a campaign aiming at informing all of their internet subscribers about the initiative.

Impact

To evaluate the impact of these short films, a study was carried out by the BVA poll institute with a representative sample of the French population – BVA questioned 1007 people of 15 years old and more during a face-to-face discussion in their residence.

The people surveyed found that the campaign is:

- legitimate (89 % indicate that it is more necessary "to protect the minors who use Internet")
- recognised (50 % indicate that the campaign is carried out on the initiative of the authorities)
- appreciated (83 % of the parents say "to have appreciated" the campaign)

The campaign was also broadcasted on the ISPs portals.

Time frame

The campaign was announced in September. Some of the activities started immediately afterwards (e.g. procurement, design, shooting) to be able to broadcast the initiative before summer and be on line with the related projects (i.e. delivery of the parental access control software in April and launching of the family label in September-October). It took eight months to develop the campaign.

Budget

Campaign budget is 1000000€ (limited for the Ministry to the realisation and broadcasting of films), plus the cost of website banners for the ministries and the ISPs.

*Summary of the 10 short films (*http://www.famille.gouv.fr/protec_enfance/*)*

Episode 1 : Le contrôle parental sur Internet (parental access control on the internet) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_1.mpg

The father has just installed parental access control software, while following the procedure suggested by his ISP and before determining the profiles of each member of the family, he discusses it with his wife and Chloé, her 12 year old daughter. They agree on the interest to be able to have protection adapted to the age of their children.

Campaign advice/ software functionalities: Definition of the profiles "children", "teens", "adult"

Episode 2 : La messagerie instantanée (Instant Messenger) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_2.mpg

Chloé, uses instant messaging: someone unknown wishes to be added to her list of contacts and sends her a message. Her mother warns her "On the Internet it is like in the street, one does not speak with an unknown"

Campaign advice/ software functionalities: Control of activity, choice of the information to be communicated.

Episode 3 : Les sites indésirables (undesirable websites) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_3.mpg

Michel (the father) and his son Yann (17) are making a search on the Internet. Yann receives a message with a link to a paedophile website. Michel proposes to his son to alert the authorities on www.internet-mineurs.gouv.fr

Campaign advice/ software functionalities: black list and white list sites.

Episode 4 : Le Blog (the blog) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_4.mpg

While updating her blog, Malika receives a comment with a link to a pornographic website with paedophile tendency. She seeks advice from Yann, her boy friend, before removing the link. They decide to alert the authorities on www.internet-mineurs.gouv.fr

Campaign advice/ software functionalities: black list and white list sites.

Episode 5 : La sécurité des paiements (payment security) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_5.mpg

The mother wants to order a ticket on the web. Her son is helping her and shows her the icon representing a lock which ensures the safety of the payment.

Campaign advice/ software functionalities:
Possibility to choose information to be communicated,
prohibition of certain personal information,
credit card number filtering.

Episode 6 : L'achat en ligne (buy on line) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_6.mpg

Chloé, the small sister, is wants to purchase a product on the Internet. She asks for a credit card from her mother. They speak about it.

Campaign advice/ software functionalities: control of activity, blocking of personal data, credit card number filtering

Episode 7 : Les données personnelles (personal data) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_7.mpg

Yann, the big brother, has just created his blog when he receives advertisements on its portable. The father explains to his son that he is not obliged to give personal information to be registered, and advises him to choose pseudo details.

Campaign advice/ software functionalities:
Possibility to choose information to be communicated, **prohibition of certain personal information**

Episode 8 : Le courrier indésirable (undesirable mail) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_8.mpg

Yann has just created an email address for his grandmother. She worries about the "spams". Her small son activates an anti-spams function.

Campaign advice/ software functionalities:
anti-spam function

Episode 9 : Chantage sur le net (Blackmail on the Internet) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_9.mpg

Chloé chats with a schoolmate she hardly knows; he asks her to send him pictures of her in a swimming suit; worried, she talks to her mother... This one explains her risks of such behaviour.

Campaign advice/ software functionalities:
Blocking of personal data, do not send personal pictures to an unknown.

Episode 10 : La Dépendance au jeu - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_10.mpg

Yann is playing his favourite game and his girl friend Malika does not manage to drag him out of it. Malika finds that he is spending too much time in front of the screen. Time flew for Yann.

Recall of the new device: activity control, deducts time spent to play.

Refer to banniere_cegetel3.gif in the *Electronic Files* section for a banner design used by ISPs and ministries for their portal.

Refer to neufkit2.jpg in the *Electronic Files* section for a window proposing the installation of parental control access software during the configuration of a new internet access connection.

Public-private partnership

Agreement between government and ISPs

On 16th November 2005, following the Conference of the family, an agreement between the Minister, the ISPs (including AOL, Wanadoo, Alice / Telecom Italia, Noos-Numéricable, Club Internet / T-Online etc.), and the family and child welfare associations has been signed. Refer to accord_afa_famille_avec_logo.pdf in the *Electronic Files* section for information on an agreement between French government and the ISPs.

ISP commitments

The ISPs committed to propose to their subscribers free parental access control software including three profiles adapted to the age of each child: "child", "teenager" and "adult".

Each profile opened or restricted internet surfing according to objective criteria for the protection of the child (for example, no shocking contents for the child profile). This system is effective since April 2006.

“E-enfance” (E-childhood), an association dealing with child protection on the Internet, is carrying out surveys and investigations directly from the ISP portal in order to check if ISPs are respecting the agreement.

Charter between Government and Mobile Phone Operators

On 10th January 2006, the mobile operators France Telecom, SFR and Bouygues Telecom signed a charter developed in collaboration with the Ministry. Refer to charte_d'engagements_des_op_contenu_multimédia-signée.pdf in the *Electronic Files* section for information on the charter between the French government and mobile phone operators.

Mobile phone operator commitments

Mobile phones operators agreed to provide a parental access control device in a systematic and free way to any new mobile phone subscriber from November 2006. Moreover, between

April and October 2006, the current mobile phone subscribers will have received three messages introducing the new safety service.

9. Germany

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Germany have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as partner with civil society

Metrics and key performance indicators (KPIs)

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

IT security is an integral part of Germany's national security strategy.

The federal government's activities focus on a framework of different aspects related to information security where awareness raising is covered as an essential issue.

At the Federal Ministry of the Interior, the federal government has adapted the structures necessary with a view to the complex requirements of information and communication technology at a very early stage.

Another measure followed at the beginning of 2002 with the establishment of the IT Staff Unit (Office of the Chief Information Officer) whose remit focuses on issues related to IT security.

Responsibilities of the Federal Government for IT security

The Federal Ministry of the Interior (BMI) and, first and foremost, its IT Staff Unit (Office of the Chief Information Officer) are responsible for IT security in the Federal Government.

The German Federal Office for Information Security (BSI) belongs to the area of competence of the Federal Ministry of the Interior.

The German Federal Office for Information Security (BSI)

BSI is the federal government's central IT security arm.

With a host of information and advisory services on offer for federal authorities, IT manufacturers and users, data protection officers, security advisers, experts, audit bodies, research institutes and standardisation organisations, the Federal Office for Information Security contributes a great deal towards improving IT security.

Whilst the www.bsi.bund.de portal offers professional users all kinds of technical and specialist information, private users can find more general information on the net at www.bsi-fuer-buerger.de

The work of the Federal Office for Information Security currently focuses on a range of topics, including, for example, critical information infrastructures, the CERT-Bund Computer

Emergency Response Team, early warning systems, fostering citizen awareness for IT security issues, Internet security, IT security management (IT-Grundschutz), malicious programs, trusted computing, development of cryptographic methods and products, certification and further development of the common criteria, secure e-government, electronic signature and biometrics.

The new National Plan for Information Infrastructure Protection

To ensure full protection of information infrastructures in Germany, the Federal Government has set out three strategic objectives in the new National Plan for Information Infrastructure Protection:

- Prevention: Protecting information infrastructures adequately
- Preparedness: Responding effectively to IT security incidents
- Sustainability: Enhancing German competence in IT security/ Setting international standards

These objectives are a supplement to the Federal Government's IT strategy. Implementation plans for the federal administration and for critical infrastructures will be drawn up to ensure that these objectives are achieved, and additional plans may follow, if necessary.

The growing importance of information infrastructures requires joint action by the state, economy and society. With the present National Plan, the Federal Government ensures that these tasks are fulfilled.

IT security in the federal administration

The federal administration itself operates parts of the national information infrastructure. The present National Plan serves to guarantee medium and long-term IT security on a high level. Therefore, the Federal Government will set out precise guidelines for the protection of the federal administration information infrastructures in an implementation plan for the federal administration (Umsetzungsplan Bund).

This plan should lay down jointly prepared technical, organisational and procedural standards for the federal administration, which the ministries should apply in a flexible manner under their own responsibility.

As the national authority in charge of IT security and as the Federal Government's main IT security service provider, the BSI is responsible for coordinating the implementation of this National Plan. To enable the BSI to fulfil this task, the number of its staff has been and to some extent still will be increased and priorities will be redefined; overall, the BSI will be assigned a more active role as IT security advising institution.

Cooperation between the federal government and the private sector

In Germany, the majority of information infrastructures are run by private companies.

Therefore, the Federal Government calls upon its partners in the private sector to take an active part in implementing the National Plan.

To this effect, the Federal Government, together with operators of critical infrastructures, is preparing the CIP Implementation Plan (Umsetzungsplan KRITIS). It will lay down measures to raise the level of IT security considerably. The BSI as well as other competent public authorities will offer their expertise to assist the operators of critical infrastructures in carrying out the measures set out in the CIP Implementation Plan.

Citizens and society as a whole

Comprehensive protection of information infrastructures in Germany is not only the business of IT specialists. It needs the commitment of everyone – of manufacturers of IT products, service providers, employees, people in charge of IT matters in public authorities and private businesses, and of those who use these structures.

As consumers, citizens increasingly use information infrastructures. In so doing, well-informed consumers are very aware of the security issues involved and therefore prefer trustworthy products and procedures. Hence, compliance with high security standards is also a positive economic factor for IT manufacturers and distributors and IT service providers; it is the basis of a functioning market and innovation schemes.

The aim of the Federal Government is to encourage people to make more intensive use of existing information and information provided in this National Plan. By following the government’s recommendations citizens actively contribute to IT security in Germany, and at the same time manufacturers and distributors of IT products and services are encouraged to give utmost priority to the security of their products already during development and adequately inform their customers of IT risks and possible protective measures.

Awareness raising as a fundamental issue for IT security

Security risks can be reduced by disseminating the knowledge about threats and possibilities for protection, by clearly assigning responsibilities for security matters, by implementing security measures and by using reliable products and processes.

Raise awareness of risks related to IT use

The Federal Government continues to trust in raising the awareness of and informing the general public and the business sector about the risks to IT use. To this effect, initiatives are being launched that are directed to people at all levels, from corporate management and high-level public administration to ordinary employees and private individuals as PC users.

Use of safe IT products and secure IT systems

The Federal Government supports the use of reliable IT products and systems and trusted IT security applications in Germany, above all within the federal administration. The Federal Office for Information Security will extend and improve its capacity to examine and evaluate IT products and systems under security aspects and issue relevant certificates. The BSI publishes best practices, lists products that were issued a German IT security evaluation certificate and issues technical guidelines for the use of these products.

The business sector is made particularly aware of the risks associated with information theft (e.g. caused by economic espionage) and the possibilities and benefits of preventing such theft by using reliable German encryption products.

Creating framework conditions and guidelines

The Federal Government undertakes efforts to create adequate framework conditions and guidelines, taking account of international norms and standards, in order to ensure full protection in all security-relevant areas.

Each federal Ministry will make sure that standards and guidelines are implemented in accordance with the Umsetzungsplan Bund by its own Ministry and all authorities within its remit, for example by putting the necessary structures in place (e.g. commissioner for IT security issues; reporting; role and responsibilities of the management, etc.).

Appropriate guidance will be given to those branches of the economy where special requirements apply to IT security. All other areas of society will be provided with recommendations and guidelines on IT security.

Identifying, registering and evaluating incidents

The IT crisis response centre at the BSI, which is currently being put in place, will play the role of a national control and analysis centre that will be able to provide a reliable assessment of the current IT security situation in Germany at any time and that will cooperate with other existing national and international crisis centres in a given incident. To enable the BSI to fulfil this function, a network of sensors will be put in place to detect IT security incidents. Additional sources supplying information on IT incidents will be made available to the BSI by extending the international watch and warning network, of which the Federal Government was a founding member. All these measures will ensure that those in charge in the public and to some extent the private business sectors have the information necessary to quickly decide what action has to be taken and can be taken.

Informing, alerting and warning

The competent federal authorities will provide information on current threats and risks tailored to certain target groups. All those in charge of IT systems and information infrastructures, from the ordinary private user to the IT administrator in companies, public authorities and other organisations, will get access to appropriate information.

As part of the national IT crisis management concept of the Federal Government, an alert and warning system will be established to inform all those potentially affected in a rapid and comprehensive manner of imminent attacks against or severe disruptions of information infrastructures. This will help respond in time and prevent large-scale damage.

IT security competence in school education and professional training

The Federal Government uses its expertise in the field of IT security to raise the priority of IT security in school education and professional training on a broader scale and to make sure that IT security is given due heed in developing new professions and training and study subjects. Furthermore, information services for citizens, schools, universities, the business sector and public administration will be expanded and improved, increasing awareness of IT security issues within society as a whole.

The BSI is closely working together with institutions in Germany that are providing material for schools and kindergarten. It was often the case that IT-security was not a part of these materials, which focused more on the pedagogical aspects of the topic. The BSI is advising these institutions to also integrate the technical aspects of IT-security and is helping them in doing so.

Legal, regulatory, and institutional arrangements to raise awareness

Refer to the start of the *Gov. as Developer* section for information.

National government as user of information systems

Recent awareness programmes and initiatives

Refer to the *Gov. as Developer* and *Gov. as Partner (Business)* sections for information.

Local government as user of information systems

Recent awareness programmes and initiatives

Refer to the *Gov. as Developer* and *Gov. as Partner (Business)* sections for information.

Government as partner with business and industry

Recent awareness programmes and initiatives

Information and guidance provided by BSI

The Federal Office for Information Security offers information and guidance both for professional users and for citizens via the www.bsi.bund.de portal.

Within the framework of the publication series of the Federal Office for Information Security the following issues are worth to be highlighted:

- IT- Grundschutz Manual / IT-Grundschutz Tool / IT-Grundschutz Guidelines / Sample Guidelines
- E-government manual
- Secure use of telecommunications equipment

For more information, refer to www.bsi.de/literat/buanzg.htm

Brochures used include:

- "Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte" (Wireless local communication systems and related security aspects)
- "GSM-Mobilfunk - Gefährdungen und Sicherheitsmaßnahmen" (GSM mobile communications – threats and security measures)
- "Bluetooth - Threats and Security Measures"
- "IT-Sicherheit Kompakt" (Concise guide to IT security)

For more information, refer to www.bsi.de/literat/brosch.htm

Study results and publications:

- Performance of penetration tests, performance of IT security inspections, intrusion detection
- Biometrics, RFID, e-government, web application security

For more information, refer to www.bsi.de/literat/studien/index.htm and www.bsi.de/literat/index.htm

Some further initiatives which deserve special mention

IT-Grundschutz

The IT-Grundschutz Manual of the Federal Office for Information Security describes standard security measures for typical IT applications and systems with normal protection needs. This manual includes:

- a description of an assumed threat situation
- detailed descriptions of measures to be taken as implementation aid
- a description of the process for achieving and maintaining an adequate IT security level
- a simple procedure for determining the IT security level achieved in the form of a target performance comparison

The implementation of the recommendations summarised in the IT-Grundschutz is in a broader sense also a precondition for systems with high and highest protection needs. The IT- Grundschutz Tool (GS tool) offered supports the development of a security concept.

Since 2003, the Federal Office for Information Security has been offering a certification system according to the IT-Grundschutz regime which enables the verification of the IT security level actually achieved. More than 100 auditors have meanwhile been licensed by the Federal Office for Information Security and are now capable of auditing on-site the technical and organisational implementation of IT-Grundschutz. Refer to http://www.bsi.bund.de/english/index.htm (English)

The IT-Grundschutz Manual is supplemented by "IT Security Guidelines" - these guidelines give a concise and generally understandable overview of the most important IT security measures.

The guidelines focus on organisational measures and on practical examples in order to highlight threats. Refer to www.bsi.de/english/gshb/guidelines/index.htm (English)

In view of a strong demand for exemplary IT security concepts, "sample guidelines and examples of concepts" were published in 2004. The publication of "examples of profiles for small institutions and medium-sized enterprises" is planned.

www.bsi.de/gshb/deutsch/musterrichtlinien/index.htm (German)

www.bsi.de/gshb/deutsch/hilfmi/beispielprofile.htm (German)

E-government Manual as the e-government IT security standard of the Federal Office for Information Security

Target groups include not just e-government co-ordinators and decision-makers at federal-government, federal-state government and municipal administration levels, but also developers of e-government solutions and interested citizens. The manual covers issues like "secure Internet presence“, "barrier-free e-government“, "encryption and signature" as well as "data-protection-compliant e-government“.

IT security guideline

The IT security guideline gives an overview of the most important IT security measures and supports the approach towards IT-Grundschutz. The guideline is primarily designed to assist newcomers as well as managers and security officers in small and medium-sized enterprises in approaching the issue of IT security.

Information on security and encryption

The "IT-Security Made in Germany – Best Practice in Secure Business Processes" brochure was published in 2004 in co-operation with TeleTrusT Deutschland e.V. and addresses experts in the fields of IT security and encryption.

This publication was presented to the public for the first time at the ISSE 2004 (Information Security Solutions Europe) which was held in Berlin in September 2004 together with the ICCC (International Common Criteria Conference) organized by the Federal Office for Information Security.

An actualized issue of the brochure is planned for the ISSE 2006 in Rome. For more information, refer to www.teletrust.de

Information for business

The Federal Ministry of Economics and Labour (BMWA) and the Federal Ministry of the Interior have initiated in 2003 the establishment of a CERT for Small & Medium Enterprises (Mcert) as a Public Private Partnership, an endeavour including several important partners from the German IT-industry.

Mcert provides an Alert & Warning Service especially focused on vulnerabilities of software products typically used in small and medium enterprises, or other threats posing a risk to them. For more information, refer to www.mcert.de

TeleTrusT Deutschland e.V.

Various projects, for example, to promote the trustworthiness of information and communication technology, are being carried out in co-operation with TeleTrusT Deutschland e.V. (TTT).

TeleTrusT Deutschland e.V. was established in 1989 as an association dedicated to promoting the trustworthiness of applications and services based on electronic signatures, authentication and encryption in an open system environment. Adequate security of information and communication equipment, services and applications whist maintaining compatibility with international standards and interoperability are the guiding principles, with innovative cryptographic and biometric methods being the path. For more information, refer to www.teletrust.de

Public Private Partnership Initiative D 21

Initiative D21 is Germany's largest public private partnership with more than 400 representatives from industry, associations, political parties, political institutions and other organisations committed to improving the framework for a quick and successful change in the information and knowledge society in order to boost Germany's international competitiveness and to better enable the country for the future. For more information, refer to www.initiatived21.de

The BSI is present at the two main IT fairs in Germany, the “CeBIT” and the “Systems”. The services and products of the BSI are presented for various target groups, including business people.

Government as partner with civil society

Recent awareness programmes and initiatives

Particularly successful initiatives are the awareness campaigns (as detailed in *the Gov. as Developer* and *Gov. as Partner (Business)* sections) launched by the Federal Office for Information Security ("BSI für Bürger" – "The Federal Office for Information Security for Citizens") as well as the security manuals and guidelines which have contributed significantly towards enhancing the overall level of IT security in Germany.

The BSI provides a range of material to inform private users on the necessity to deal with the topic of IT-security in their "private life". Also it provides tools to support users. 2 best practice examples in awareness raising:

- www.bsi-fuer-buerger.de: The website informs the private user on all issues concerning IT-security. It is written in an easy-to-understand language, so the non-professional is able to understand and use the provided tips and checklists. Also free tools, such as anti virus protection, personal firewall etc., can be downloaded from the website. The contents of the website is also distributed on a CD-Rom e.g. at trade fairs or at events. Also co-operations with big companies have been established to use BSI material for awareness raising among their employees
- www.bsi-fuer-buerger.de: Portal for private PC users was implemented in 2003. The information offered there is additionally distributed through various channels to millions of users

Bürger-CERT (www.buerger-cert.de) - the first CERT for citizens in Germany: Private users can sign up for up to three different alert-services (due to their individual demand of protection).

1. The newsletter "SICHER ° INFORMIERT". Since the end of 2004 this newsletter provides up-to-date information from the BSI on viruses and general aspects of IT security for all citizens
2. Technical Warnings ("Technische Warnungen") for citizens with technical knowledge
3. The Special edition of the "SICHER ° INFORMIERT"-Newsletter. In any case of a great risk for users which allows no delay

Furthermore citizens are warned when critical security issues arise and also will be provided with a guideline on how to deal with these risks (e.g. where to get a patch etc.).

Refer to the *Gov. as Partner (Business)* section for information on other German initiatives.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

Various methods adapted to the particular purpose in question are in place in order to check and verify IT security systems and assess the effectiveness of the federal government's IT security and awareness initiatives.

Penetration tests

Penetration tests are carried out in order to determine to what extent the security of IT systems is vulnerable to threats from hackers, crackers, etc. and/or whether the protection measures taken actually ensure the security of a given IT system.

The Federal Office for Information Security operates its own penetration centre for this purpose.

The activities of the IT penetration centre of the Federal Office for Information Security are currently focused on checking the security of Internet applications within the framework of the BundOnline 2005 initiative and on auditing the Berlin-Bonn Information Network (IVBB).

Federal Office for Information Security surveys

Studies of future developments and trends in the fields of information technology and information security are prepared within the framework of trend analyses.

They serve as a basis for the general definition of future political decisions related to IT security and for the identification of future baseline activities by the German Federal Office for Information Security.

Once a year, monitoring is performed with a view to awareness for the products of the Federal Office for Information Security. IT security officers, data protection officers and journalists are polled in representative surveys.

In 2004, "awareness monitoring" was also carried out among the target group of private PC users in this context. The results are considered within the context of project planning by the Federal Office for Information Security. Polls among experts and citizens are also planned for the future.

10. Greece

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Greece have been detailed:

Current Situation

Campaign Initiatives

Current Situation

The SafeNetHome report states that:

- Over 50% of Internet users have a virus checking program or a firewall. Problems actually met on the Internet are mostly spam and computer viruses, with percentages under 1% of cases dealing with credit card or personal information abuse
- The situation is not the same concerning Internet safety: 92% of the Greek families state the need to be more educated on how to protect the children from illegal and harmful content on the Internet, placing Greece on rank 1 among all 25 EU member states
- According to the most recent Eurobarometer survey[3], Internet usage among children is still rare in Greece (15%): 7% of the children surf from home, whereas 8% surf from their school, placing Greece at the bottom of the list among the 25 EU member states
- Most Greek parents expect the mass media to educate them about the appropriate usage of the Internet (43%), with all other alternative information sources lying far behind (ISPs follow with a percentage of 19%). Among the desired ways of getting information, TV is placed on rank 1 (66%, the highest percentage among EU-25), followed by newspapers (37%) and the radio (31%)

Campaign Initiatives

SafeNetHome

The Greek awareness node "SafeNetHome"

SafeNetHome, http://www.saferinternet.gr/ , is the Greek node for public awareness against harmful content distributed through the Internet and other New Media. SafeNetHome is a member of Insafe (http://www.saferinternet.org), a network of 23 awareness raising nodes in 21 countries that coordinate Internet Safety awareness in Europe.

The goal of SafeNetHome is the design and implementation of a hard-hitting awareness campaign in Greece for different target groups about the potential dangers lying in illegal and harmful content on the Internet but also in mobile and emerging technologies. The campaign has been implemented based on the slogan 'Saferinternet … together', thus inviting every member of the society to contribute in making the Internet and all new technologies safe for all consumers, but especially for kids and youngsters. The campaign focuses on parents, educators and kids, but is also addressing public authorities, the government and the media.

The Safer Internet awareness campaign for Greece

Given the fact that Internet integration in every day life in Greece is still in its infancy, the country is grabbing the opportunity to build on knowledge and experience gained, foster cooperation with key players and stakeholders, and build the public's confidence on the benefits of the new technologies. The aim is to highlight the key for the optimal and safe use of media, bridging the gap between generations, interconnecting existing initiatives, and exchanging information, tools and methods with other European awareness nodes.

According to the latest Eurobarometer survey, the Greek public prefers TV, radio and the press for getting information about safer use of the Internet. For that reason, the campaign is built upon a "frontal attack" on TV, radio and the press, accompanied by a "flank attack" covering a very informative Web portal in the Greek language for youngsters and adults, and diverse electronic and printed awareness & training material.

Parallel to the above activities, a series of open events for educators, parents, children and youngsters has been organized, with the most important event being the yearly celebration of the "Safer Internet Day" in cooperation with InSafe and all other national awareness nodes.

Refer to safenethome_annualreport2005.pdf in the *Electronic Files* section for more information on the SafeNetHome campaign initiatives.

The "SafeNetHome" consortium

The work of the SafeNetHome project is implemented by a consortium of two Greek entities, closely working together for Internet safety awareness since 2000: The Hellenic Consumer Organisation E.KAT.O., and Extreme Media Solutions Ltd.

For more information on the consortium, refer to
http://www.saferinternet.gr/Default.aspx?PageContentID=88&tabid=105

11. Hungary

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Hungary have been detailed:

Current Situation

As of April-May 2006, Hungary has undergone parliamentary elections, which had an effect on current government initiatives. All strategies, frameworks, programs and plans included in this report reflect the activities of the previous government. The organisational structure of the new government is presently under formation, and new strategies and programs are likely to be communicated in September-October 2006.

Past and running regulations and initiatives as well as concepts for the near future have been included where applicable.

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

41/2001 Government Regulation, amended in 2003, declared the Ministry of Informatics and Communications (IHM – www.ihm.gov.hu), as the European Center for information related topics. In 2003-2004, the establishment of CERT-Hungary, the government CERT of Hungary took place, and the responsibility shifted to CERT-Hungary. To comply with the general awareness role, CERT-Hungary has set up two information websites, one for general public regarding internet security, www.biztonsagosinternet.hu, and the other for network safety, www.halozatbiztonsag.hu, mainly for network administrators. Other than this, CERT-Hungary operates its own website, disseminating all vital and approved vulnerabilities and threats.

There are two inter-ministerial committees dealing with ICT related subjects, one is the ITKTB (Inter-ministerial Committee on Information Society – www.english.itktb.hu/Engine.aspx), that cooperates in processing the Hungarian Information Society Strategic and Action Plan. The other is the KIETB (Inter-ministerial Committee on e-Government – www.meh.hu/szervezet/hivatalok/ekk/kietb/kietb20041116.html), set within the Ministry of the Prime Ministers Office, handles all issues on safe and secure e-Governance.

The new IT strategy, including awareness raising will be coordinated within the Ministry of the Prime Ministers Office.

Legal, regulatory, and institutional arrangements to raise awareness

IHM has backed all major programs that have dealt with awareness raising, including Hungarian and EU action plans, as well as cooperation with enterprises and civil bodies. Regulatory authorities, such as the National Telecommunications Authority (NHH – www.nhh.hu), have undertaken measures concerning spam measurement, awareness raising and filtering (www.spam.baratsagosinternet.hu). I.e. the last Safer Internet day has been dedicated to battling spam.

National government as user of information systems

Recent awareness programmes and initiatives

There is one general national government system; the electronic portal of Hungary, www.magyarorszag.hu. The portal is for the benefit of the Hungarian citizens, but also involves the competence of civil servants to make efficient use of the portal. There has been a widespread media campaign to promote the use of the portal, as well as good training for the operators.

The aforementioned KIETB also takes up the role of public awareness raising in the field of the continuously developing e-Government system. Its recommendations on the functions and procurement of the elements of the portal also come in line with the security aspects of the end users.

Another initiative for the promotion of network security comes in the form of CERT-Hungary's consultancy role with its constituency. Being a government CERT, the main clients include some parts of the critical information infrastructure of Hungary, such as:

- Civil Aviation Authority of Hungary
- Ministry of Informatics and Communication
- National Communications Authority
- NETI Ltd.
- NT Public Beneficiary Ltd.
- Public network
- Theodore Puskas Foundation

The information channel to raise awareness includes weekly newsletters and public information on CERT-Hungary's homepage.

Local government as user of information systems

Recent awareness programmes and initiatives

It is difficult to measure the awareness programmes of local governments, as the municipal system is very fragmented, and every local government can have their own information systems. However, there are some programmes aimed at educating security at a very local level. There is the Telehouse network (www.telehaz.hu) which makes internet and computer literacy more widespread, and the IT mentor program (www.itmentor.hu) to raise awareness among users at local level.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

In 2005, the IHM started an initiative to bring together significant IT security SMEs, under Hungarian ownership, called eSec.hu (www.esec.hu). The members of the group each represent a different field of IT security, covering the whole area, such as:

- Kürt Ltd. - data recovery, data protection
- BalaBit Ltd. - firewalls, content filtering
- VirusBuster Ltd. – virus & spam protection
- Megatrend Ltd. – business information systems
- E-Group Ltd. - PKI, document protection
- CERT-Hungary – incident handling, advisory, training

The group of companies formed a consortium in 2006, with a common interest, namely:

- joint EU and Hungarian tendering
- representation of common interest in the field of IT security
- influence and advisory to policy makers
- sustain profitability in EU ground

The eSec.hu consortium is a profit oriented venture, however, there is close link to public awareness programs, as one of the members is CERT-Hungary. Many of the proposed tenders are 'awareness' related, such as Safer Internet+, or eContent, where future collaboration is desired among the partners.

Internet Service Providers (ISPs)

ISPs have a great responsibility in creating awareness among users. They have their own association (www.iszt.hu/iszt/English) to represent their interest with policy makers. First step to raise awareness on a common basis with the government is to have statues on self regulation. The organisation to coordinate communication between government and ISPs is Hun-CERT, the industry and ISP CERT of Hungary.

As of now, there has been no joint awareness programs aimed at the public. CERT-Hungary and Hun-CERT work in good relationship, and as part of this work, an exercise has been carried out to check on the tendency of ISPs to cooperate in the field of IT security. The results are expected to be communicated in the fall through different channels, targeting specialized media as well as general public.

Media

It should be noted that the examples listed below use media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

General printed media has not yet picked up on IT security issues as much, so basic awareness raising initiatives have been the topic of specialist media so far. As internet media is gaining ground, it is important to set up informative websites on IT security, and publicize them. This task has been partly taken up by CERT-Hungary, with the operation of two IT security websites. One for general public about internet security, www.biztonsagosinternet.hu, and the other for network safety, www.halozatbiztonsag.hu, mainly for network administrators

There are several privately owned publications which are specialized for the ICT market, such as IT business (www.it-business.hu) or Connect magazine (www.connectmagazin.hu). Other magazines include Chip (www.chiponline.hu) or Linuxvilág (www.linuxvilag.hu), etc, but their relevance in awareness raising is basically narrowed down to commercial interest.

Not so closely related to the Media sector, but worth mentioning is the conference activities of Hungary in the recent years. There have been several upscale events in Hungary, such as FIRST Conference in 2004 and the ISSE Conference in 2005. Both events received good media coverage, and 2006-2007 is also to host some major specialist events.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The best example for awareness raising in public-private partnerships (PPP), is the eSec.hu consortium (as mentioned previously). The members of the group hold a wide range of the IT security spectrum, and are committed to create a secure IT environment both in the public and private sector. The cutting edge solutions are used by the government, the public administration, the academia, commercial companies, as well as the general public users.

One example of the activities of the PPP is a charity type conference for the implementation of ISO 27000 standard, where all members of eSec.hu could contribute to its promotion.

A major aim of the eSec.hu consortium is to lobby for the creation of a law that standardizes the use of PPP in the field of IT security.

Government as partner with civil society

Recent awareness programmes and initiatives

Government and civil societies are undertaking several collaborations in the field of awareness raising for the protection of home users and general public.

One forum to create the common interest with all parties is IT KTB (Interministerial Committee on Information Society), established on 25th February 2003 after the government decree 1214/2002, www.english.itktb.hu/Engine.aspx. The main task of the committee is to consult on the matters of the National IT Strategy, where the main issues are delegated to the subcommittees of each field. Civil societies are part of the discussions as well.

KIETB, the Interministerial Committee on e-Government, created by the government decree 1054/2004, also includes several non-governmental members, as permanent consultancy delegates. This allows wider discussion on the aspects of secure and user friendly e-Government portals.

Another main sector forum, where government is actively present in discussion of IT security issues, is the Association of Hungarian IT Companies (IVSZ, www.ivsz.hu). IVSZ is involved in several EU initiated projects, which are partly IT security and awareness raising related, e.g. IT mentor or Secure-Force.

The IHM also played an active role in fostering several awareness raising initiatives with civil societies. The EU Safer Internet program started several ongoing projects in Hungary, that that are partly managed or supported by the former Ministry. Some of these include the Hungarian Internethotline (www.internethotline.hu) in collaboration with MATISZ (Hungarian Association of the Content Industry, www.matisz.hu) and the cyber-crime division of the police (National Bureau of Investigation). The Internet hotline is already an accredited member of the INHOPE network. Another of these actions is the site labelling activity to raise awareness among young children and parents. MTE (Hungarian Content Providers Association – www.mte.hu) is nurturing the Hungarian Safer Internet site (www.baratsagosinternet.hu), in cooperation with MATISZ, INFORUM (www.inforum.org.hu), IHM, and CERT-Hungary.

Some actions that are going to take place in the near future in collaboration with civil societies include a joint action plan with CERT-Hungary and MATISZ (Hungarian Association of the Content Industry, www.matisz.hu) to bring a training course to life in the telehouse network to educate IT security issues, based on the material publicized on www.biztonsagosinternet.hu, following the example of the BMI, Germany on www.bsi-fuer-buerger.de. This material is created in such a way that it is easily understood by home users, children and parents. A further aim is to be able to reach schools, and have an influence on young users concerning security related issues. This idea comes in line with the ambition that IT literacy, including IT security, will have to be part of the national curriculum.

Another direction of awareness raising and education in the field of ICT is the cooperation between ISACA Hungarian Chapter and CERT-Hungary, where different levels of curriculum are being assembled to be able to provide trainings at various levels of ICT competence. CERT-Hungary will be able to provide lectures for ISACA credits for CISA, CISM certified professionals, but also, the vast amount of joint literature will create a basis for any form of education. The lobby power here is also to make IT security part of the national curriculum.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

As of now, there are no KPIs available for assessing the awareness initiatives.

There is need for a common way of performance measurement, but the national characteristics have to be taken into account when comparing different Member States.

12. Iceland

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Iceland have been detailed:

Campaign Initiatives

Campaign Initiatives

SAFT (Samfélag, fjölskylda og tækni) is an awareness project run by Heimili og skóli – The National Parent's Association in Iceland (November 2005 - June 2006)

Introduction

Heimili og skoli – The National Parent's Association - is the internet safety awareness node in Iceland. The project is called *SAFT – Samfélag, fjölskylda og tækni* (Community, family and technology). The project is part of the INSAFE network of European awareness nodes, under að contract from the Safer Internet Programme of the EU. The projects acronym is SIAPI (Safer Internet Action Plan Iceland) and the project's term is 1st October 2004 – 30th September 2006.

During the period November 2005 to June 2006, awareness work has been undertaken on several fronts such as mobile phone safety, computer games and safe and ethical use of the internet. Networking is an important part of awareness work and there has been fruitful cooperation with several different stakeholders.

The main milestones during this period are:

- November 2005: A brochure for parents on mobile phone safety. (In cooperation with Og Vodafone in Iceland)
- November-December 2005: Computer games and the PEGI rating system: A brochure for parents and a media campaign (with cooperation and support from SMAIS –The Association of Film Rights Holders in Iceland, The Ministry of Education, Microsoft and Gallup)
- February 2006: Safer Internet Day 7th February. A conference and blogathon on the SAFT website (www.saft.is) on Ethics and the Internet
- June 2006: A guiding card for parents with 10 advices on mobile phone safety and 10 advices on internet safety (in cooperation with Siminn (Iceland Telecom))
- March-June 2006: Design of a media campaign on net-ethics to be run in August-September, design of two education modules for schools on net-ethics and source criticism to be distributed in September. Also, a revision of the brochure for parents on mobile phone safety to be distributed in August-September

Apart from the milestones above there is an active website, www.saft.is; also meetings with parents and stakeholders are an important feature in the work.

1. A brochure for parents on the safe use of mobile pones

"Foreldrar börn og farsímar" (Parents, children and mobile phones) is the title of a brochure for parents on mobile phone safety that was published in cooperation with Og Vodafone in November 2005. The first copy of the brochure was given to the Minister of Education in Iceland at a press meeting on 1st November. It has been distributed at SAFT meetings with parents and in the shops and service centers of the Og Vodafone company.

The brochure is being revised after a survey done in May 2006 and will be re-published and widely distributed in August-September 2006.

2. Computer games campaign (November-December 2005)

A campaign to raise awareness of computer games and the PEGI rating system was run in November and December. The campaign was planned and managed by SAFT with support from the Ministry of Education, SMÁÍS – The Association of Film Rights Holders in Iceland, PEGI, Microsoft in Iceland and Gallup:

- **Survey among children age 9-16 on computer game use** was conducted for SAFT in September by Rannsóknir og greining (The Icelandic Centre for Social Research and Analysis). The survey was done with the cooperation of schools and the children answered the 20 questions of the questionnaire in the schoolroom. The sample was chosen by random and the answering percentage was 90%
- **Survey among adults** on the knowledge on the PEGI rating system was done in September 2005 and again in December, i.e. before and after the campaign. It shows a 35% increase in the knowledge of the PEGI rating system among those who said they bought computer games
- **A brochure** for parents on computer games and the PEGI rating system (see picture) was designed, printed and distributed to parents of all elementary school children in the country, 45.000 in all. The text was based on the children's survey and information on the PEGI rating system. The distribution was done in cooperation with all elementary schools in Iceland who sent the brochures home with all their students
- **An animated advertisement**, titled "For whom is the computer game?" was designed and shown in film theatres and on the main television stations during the

running of the campaign. Film theatres were showing it from 7th December to 10th January. It is still being used occasionally on the television stations

- **A slide advertisement** was designed and shown in film theatres and television during the period 7th December to 10th January. It is still being shown occasionally on the main TV stations
- **An advertisement banner for buses** was designed and visible on 20 buses in the capital city of Reykjavik from 26th November through December and well into January.
- **Four kinds of web–banners** were designed and widely visible on common Icelandic websites
- **Newspaper articles:** Articles by staff on computer games and ratings were written and published in the main newspapers in Iceland

The success of the Computer game campaign was assessed by doing a survey on the knowledge of the PEGI rating system before and after the campaign. The survey was done by Gallup among 16 – 75 year olds, first in September and again in December. It showed a 35% increase in awareness of the PEGI rating system among those who said they bought computer games.

3. Safer internet day 2006 – SAFT conference on ethics and the internet and blogathon.

SAFT held a half –day conference on *Ethics and the Internet* on Safer Internet Day, 7th February 2006. At the same time a blogathon on ethical use of the internet was launched on the project's website www.saft.is .

The conference advertised for the general public and invitations were sent to people within the education system, governmental agencies and ISPs. Five hundred invitation cards were printed and distributed before the conference. They were also widely distributed by e-mail. Advertisements were placed in newspapers and web banners published on several websites, among them popular blogsites such as www.folk.is which is widely used by young people in Iceland.

One hundred guests attended the conference which was also streamed live on the website www.saft.is. The website showed over 30.000 hits during the day. A teacher and students of multimedia in Flensborg high school helped with the technical side of recording and broadcasting. Og Vodafone managed the streaming through the website.

The Minister of Education in Iceland, Mrs. Thorgerdur Katrin Gunnarsdottir opened the conference and launched a week long blogathon on net–ethics on the website, www.saft.is at the opening. The blogathon was presented and introduced to all schools and in the media beforehand and there was hope of a good participation on different levels. Although there was some fruitful discussion on the blogsite, the number of participants was not as expected.

Apart from the advertisements, the conference and the issues discussed got a lot of media attention in Iceland on 7th February and during the following days. All main news media in the country reported on the conference and both SAFT staff and speakers were interviewed in newspapers and on television and radio.

The conference and the following media attention sparked a discussion in the society as a whole on the matter of ethical and safe use of the internet. Both phone calls from people seeking advice and assistance and visits to the SAFT website increased dramatically around the conference.

Isabella Santa from ENISA was the key speaker and four other specialists made speeches on the issue. The conference ended with a panel discussion led by Þorbjorn Broddason, professor of sociology and media studies at the University of Iceland. The participants represented ISPs, media, government and parents.

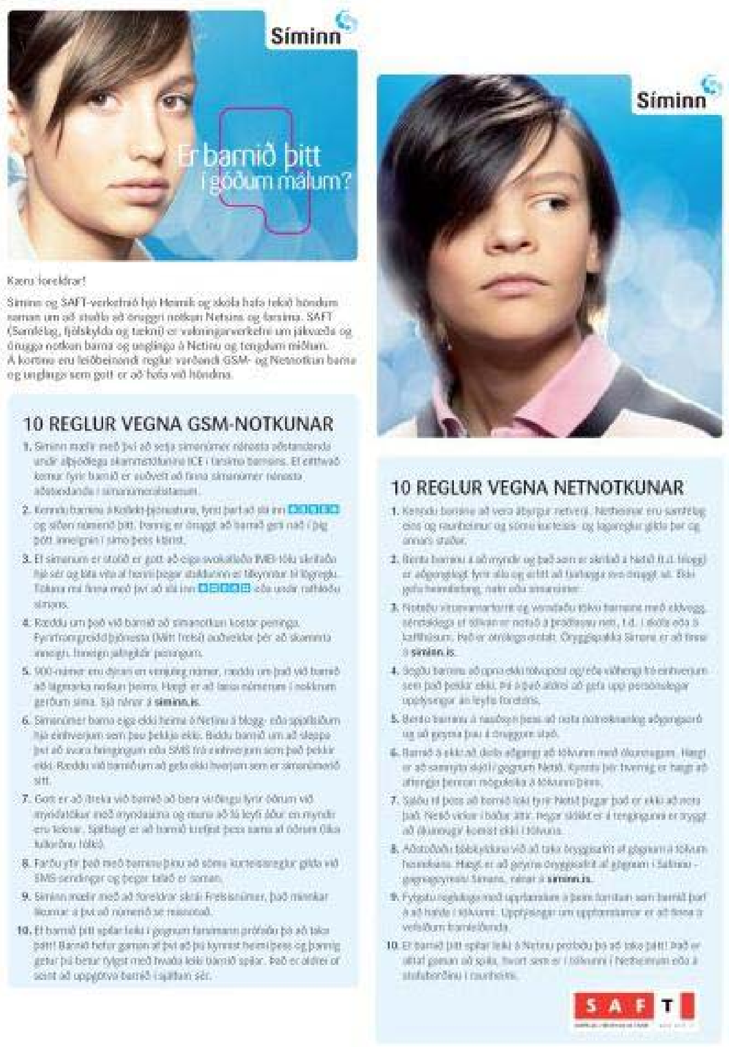
The general conclusion of the conference was to point out the need for an ongoing awareness work to reach different levels of society. The speakers all emphasized the fact that parents had a key role in teaching their children how to use the internet in a safe and positive way, as most of their “free” internet use goes on in the home.

4. A Guiding card for parents on mobile phone and internet use

On 15th June 2006 a guiding card for parents on mobile phone and internet use was launched at a press meeting and the day after it was distributed by post to parents of all 6 – 14 year olds in Iceland.

The two sided card has 10 points of advice on mobile phone use on one side and 10 points of advice on internet use on the other.

The guiding card is a joint project of SAFT and Siminn (Iceland Telecom)


Síminn
Er barnið þitt í góðum málum?
Síminn
SAFT

Kæru foreldrar!

Síminn og SAFT-verkefnið hjá Heimili og skóla hafa tekið höndum saman um að stuðla að öruggri notkun Netsins og farsíma. SAFT (Samfélag, fjölskylda og tækni) er vakningarverkefni um jákvæða og örugga notkun barna og unglinga á Netinu og tengdum miðlum. Á kortinu eru leiðbeinandi reglur varðandi GSM- og Netnotkun barna og unglinga sem gott er að hafa við höndina.

10 REGLUR VEGNA GSM-NOTKUNAR

1. Síminn mælir með því að setja símanúmer nánasta aðstandanda undir alþjóðlega skammstöfunina ICE í farsíma barnsins. Ef eitthvað kemur fyrir barnið er auðvelt að finna símanúmer nánasta aðstandanda í símanúmeralistanum.
2. [illegible]
3. [illegible]
4. [illegible]
5. [illegible]
6. [illegible]
7. [illegible]
8. [illegible]
9. [illegible]
10. [illegible]

10 REGLUR VEGNA NETNOTKUNAR

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]
5. [illegible]
6. [illegible]
7. [illegible]
8. [illegible]
9. [illegible]
10. [illegible]

4. Awareness work planned for August and September 2006

a) AUGA – Media campaign on net-ethics

A big media campaign on net-ethics, targeted at children and young people is being designed and will be run in the end of August. SAFT was chosen to receive a grant from the AUGA fund in the form of a media campaign.

AUGA (AD-AID) is a fund formed by the Society of Icelandic Advertising Agencies in collaboration with the largest media companies in Iceland, IMARK (Association of Icelandic Marketing Professionals) and with SAU (Association of Advertisers). Ad-Aid is aimed at assisting non-profit organisations promoting their cause.

b) Education modules on net-ethics and source criticism

Two education modules, one on net-ethics and another one on source criticism are being designed. They will be distributed to all elementary schools in Iceland in September and will also be accessible on the projects website www.saft.is

The education module on net-ethics will be in two parts, for ages 9-12 and for ages 13-16.

The module on source criticism will be designed for ages 13-16.

13. Ireland

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Ireland have been detailed:

Campaign Initiatives

Campaign Initiatives

Refer to the *Good Practices by Target Group Local Government* section for details of awareness raising initiatives by VigiTrust, a private organisation.

Information on awareness raising programmes conducted by the Irish Government, Ministries or any of the public organisations was not supplied.

14. Italy

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Italy have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with civil society

Campaign Initiatives

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

Main Initiative

At the end of March 2006, the National Plan for Public Administration (PA) ICT security was published, as well as the National Organisational model for ICT security in the PA. Both publications are available at www.cnipa.gov.it/site/it-it/La_Documentazione/Pubblicazioni/i_Quaderni/, in the "I Quaderni", nb 23, March 2006.

The two documents were elaborated by the National Technical Committee (www.cnipa.gov.it/site/it-it/Attivit%c3%a0/Sicurezza_informatica/) devoted to identify the national strategy for implementing suitable ICT security in the PA.

The awareness raising initiatives play a central role in the above strategy. In particular, an awareness and formative campaign has been set up with the main goal to disseminate ICT security best practices in the PA.

Three main target groups were identified:

- Top Management. For the Top Management, a one day classroom seminar was set up, covering all general ICT security aspects (legal, semi-technical, budget related) that are under their responsibility. The seminar has already been erogated to the 60% of PA top managers
- Top ICT security manager. For this set of user, a one week classroom seminar is planned, covering detailed technical and organisational aspects of ICT security. One of the goals of these seminars is to prepare the top ICT manager to be, in his turn, "teacher" of ICT security for his employees. The seminars will start within second quarter of 2006. The number of people to be reached by this formative initiative is of the order of several hundred
- Final user (i.e. PA employees). For the final user, a web based e-learning programme is under development. It is planned to reach about two hundred thousand people. The initiative is planned to start at the end of 2006.

Furthermore, there are plans to produce about 50 hours of ICT security "lessons" to be transmitted by a DGTV national broadcasting channel. The main target group of these "lessons" is the citizen with low to medium knowledge of ICT tools. These "lessons" will be watched, on a voluntary basis, also by the PA employees during working hours.

National government as user of information systems

Recent awareness programmes and initiatives

Refer to the *Gov. as Developer* section for information.

Local government as user of information systems

Recent awareness programmes and initiatives

Refer to the *Gov. as Developer* section for information.

Government as partner with civil society

Recent awareness programmes and initiatives

Information Security Citizen Awareness Initiative

The “Master in Sicurezza dei Sistemi e delle Reti Informatiche per l’Impresa e la Pubblica Amministrazione” of the University “La Sapienza” of Rome and the “Consorzio Interuniversitario per le Applicazioni di Supercalcolo per Università e Ricerca” (CASPUR), in collaboration with the “Centro Nazionale per l’Informatica nella Pubblica Amministrazione” (CNIPA), are planning to launch a novel initiative to promote awareness raising about information security in Italy.

Following the traces provided by the ENISA’s “Information Package: Raising Awareness in Information Security - Insight and Guidance for Member States”, the partnership between CNIPA, CASPUR and the “Master in Information Security” is aimed to realize a multimedia project to broadcast guidelines for a conscious and secure utilization of the Internet, as a useful instrument for news, entertainment, communication and other useful and diversified services. Notably, the project is meant to fill the gap between citizens and new technologies, documented in other ongoing projects.

The contents of the project will be organized as a real and effective educational course, freely accessible from institutional organisation web portals, such as the web sites of the CNIPA, http://www.cnipa.gov.it, and the Ministero per l’Innovazione e le Tecnologie, http://www.italia.gov.it

The topics of the course will be subject to continuous revisions and additions, as required by the dynamic world of ICTs. In the future, the course is scheduled to be available also via other media, as free CD-Rom or books.

The initiative has been started in May, and a prototype is planned to be ready for the first weeks of coming August.

The target group of the project is the Adult category of Home Users, as specified by the ENISA’s Information Package 2005, i.e. citizens born after the 1950s and older than 16 years. The target group is characterized by a diverse range of skills and knowledge of ICTs, exhibiting needs and interests such as:

- Online payments (e-commerce, bills, banking…)
- Music and software download
- Online entertainment

- Surfing in Internet for news, hobbies, organisations, products

In order to cope with the issue of a diverse range of technical skills that can range from “none” to “high”, the project organizes the topics of the course in different levels of detail: from a simple introduction for novice users, up to technical detailed explanations for most skilled users. Following the main course, each topic can be deepened, leaving the user to choose whether to go into the subject more thoroughly.

The contents of the project will space out and cover the main topics of ICTs, from accessing the Internet through to the protection of a personal computer via antivirus, personal firewalls and anti-malware tools. The important message of a continuous update to all software components of a PC, from the operating system through to the list of new viruses and malwares, will be explained. A part of the project will focus on authentication and digital signatures, as well as digital certificates and smartcards. Another section will depict the typical threats of the Internet, and the corresponding countermeasures to protect the PC. Instant messaging, peer-to-peer file-sharing and web communities will be covered as well. Finally, there will be a section related to the legal aspects of web browsing, as well as the legal guarantees of certified email, as well as the government bodies in charge to aid the citizen. A glossary will be included collecting all the terms used. Also, a motivated list of guidelines and best practices aimed at a good use of Internet will be provided.

The presence of a governmental partner such as CNIPA assures a high degree of visibility to the project and appears to be an enabling factor for the success of the initiative.

Refer to the *Gov. as Developer* section for more information on other initiatives.

Campaign Initiatives

SaferInternet - Minors & the net (article)[12]

Summary

On 19th November 2003, the Italian law on "internet and minors" was signed. It was the outcome of collaboration between the Ministry of Communications, internet industries and associations involved in the protection of minors.

Details

These bodies worked together in thematic sub-groups for the most important endeavour in Italy to date to define standards and common tools for guaranteeing the protection of minors on the internet. The law was signed by the main Italian ISP Associations.

Special focus was given to safe surfing-tools for minors, in particular filtering systems. For the first time an attempt was made to systemise and classify existing tools by rating their efficiency. This was done by providing a series of indicators on the possible contexts of use.

Naturally, the law does not only provide information: it also compels the signatories to equip themselves with differentiated and distinguishable navigation systems to be put at the disposal of families, teachers, schools, libraries, etc.

After three years, it seems that only a few ISPs have implemented the directive due to financial reasons or because restricting navigation may be interpreted as an attempt against freedom of expression. In any event, this problem is cultural and not easy to resolve. The general trend consists in providing parents and educators the tools to intervene through a proliferation of blocking systems at control-panel level or through the creation of white and/or black lists.

Some Italian Regions have introduced such systems in order to regulate the widespread internet access in schools and libraries. However, there is not enough instruction on how to use these tools. Guidance and education are necessary to help children build confidence and the ability to judge.

[12] http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0606/it1.htm, 12th June 2006.

15. Latvia

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Latvia have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as partner with civil society

Metrics and key performance indicators (KPIs)

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

There is no national strategy developed calling for enhancing awareness regarding the increasing number of information security breaches and threads.

Legal, regulatory, and institutional arrangements to raise awareness

There are different legal, regulatory and institutional arrangements to raise awareness in Latvia.

There are implemented legal provisions of the Council of Europe Convention on Cybercrime into the Latvian Republic Crime Law, such as paragraphs: 241. Unwarranted Access to the computer system; 242. Unlicensed acquiring of computer software; 243. Damaging of computer software; 244. Distribution of computer viruses; 245. Violating the security rules of the information system.

A Cybercrime department which deals with affairs in this field has been also established. This department is subordinated to the State Police.

With decision n. 684 of the Cabinet of Ministers, the Latvia's National Lisbon programme 2005-2008 sub-chapter "2.1.3. Information society" has been adopted on 19th October 2005. The programme aims at ensuring the safety of networks and information, its coherence and interoperability to form the space of information without frontiers, including:

- The development of safe electronic signature systems, improving the safety of information and broadening the usage of e-services
- The development of government and private computer emergency response teams

On 18th October 2005, the Cabinet of Ministers established the implementation plan of using a safe electronic signature carrier with a safe electronic signature.

On 25th May 2006, a draft of regulation of he Cabinet of Ministers "Procedure, how institutions place information in the internet" has been prepared and made public. In the draft of the regulation, the web page technical parameters and safety requirements have been included.

Moreover, an Electronic administrations development programme 2006 – 2009 has been accepted. One of the programme's basic principles is safe government's electronic services.

“The Latvian Republic electronic communication sectors guidelines implementation programme from 2004 to 2008” includes the development of a Computer Emergency Response Team which would collaborate with the European Network and Information Security Agency.

The Ministry of Transport is planning to strengthen rights of national regulatory authority to set appropriate regulations for publicly available electronic communications service providers to safeguard security of their services.

National government as user of information systems

Recent awareness programmes and initiatives

There are not any recent awareness programmes and initiatives.

There is the plan to implement the project “Information and communication technology infrastructure and services” with the support of the European Regional Development Fund. Within the framework of the project, significant investments will be made to ensure safe information transmission between government and institutions.

Local government as user of information systems

Recent awareness programmes and initiatives

There are not recent awareness programmes and initiatives or any plans to develop any in the near future.

Government as partner with business and industry

Recent awareness programmes and initiatives

There are not recent awareness programmes and initiatives or any plans to develop any in the near future.

Public-private partnership

No public-private partnerships have been established and there are no current plans to set-up some in the near future.

Government as partner with civil society

Recent awareness programmes and initiatives

The Secretariat of Special Assignments of the Minister for Electronic Government Affairs with the support of the European Commission has developed the Latvian Insafe nets awareness node within the framework of the program Safer Internet Plus. The node has been established in collaboration with the Latvian Internet Association.

The activities of the awareness node will kick-off in September 2006. The following tasks have been identified: examining awareness of safe internet usage in Latvia, researching youth, teachers and parents, providing training and informing the society (especially the youth, teachers and parents) about the safe usage of the internet.

The duration of the project will be of 24 months.

Public-private partnership

No public-private partnerships have been established and there are no current plans to set-up some in the near future.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

At present, metrics and KPIs haven't been identified as awareness raising initiatives haven't been developed yet. With the development of such programmes, measures will be developed to measure the success of these initiatives.

Importance of Metrics/KPIs

It is recognised that the development of common metrics and/or indicators is essential to measure the effectiveness of different awareness raising programmes within the community.

16. Liechtenstein

No information was supplied.

17. Lithuania

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Lithuania have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Government as partner with business and industry

Government as partner with civil society

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The national strategy of IT security "The Governmental strategy for IT security" was signed on 22nd December 2001. The Ministry of the Interior was responsible for ensuring the realisation of the project objectives. One of the main goals of this strategy was to improve the culture of IT security of public officials. Other State institutions were also motivated to ensure the IT security education of their public officials. In order to achieve this objective, two phases were implemented. The first phase prepared specialists of IT security and took place during the second quarter (Q2) of 2003. As a result, fifteen specialists received the international security certificate. The second phase was to organize seminars and was scheduled for Q2-Q4 of 2002 and Q3 of 2003.

A new Governmental strategy for electronic data security is now in place and set to run until 2008. Special attention is given to raising a culture of IT security. Considering that fact, that it is impossible to ensure IT security through only the efforts of a few State institutions, it is also necessary to pay attention to raising the culture of electronic data security in the private sector.

The relevant supporting material can be found on the websites www.esaugumas.lt and www.vrm.lt (in Lithuanian only).

Legal, regulatory, and institutional arrangements to raise awareness

The project "Strengthening capacities of authorities dealing with IT and Data Security" was implemented using PHARE funds in 2005.

The Information Policy Department of the Ministry of the Interior was managing the project. The following objectives were identified:

- Increase administrative and operational capacities of state institutions working with IT and data security
- Align Lithuanian IT and data protection system with the Acquis and international requirements
- Ensure proper IT and data security level

The following results were achieved:

- Laws and other legislative documents in IT and electronic Ddta security sphere were reviewed and necessary drafts prepared
- Methodology on IT and electronic data security evaluation (risk analysis) accepted and published
- Draft of security requirements for IT and Electronic data were presented to the Ministry of the Interior
- Draft of security requirements for secure governmental network presented to the Ministry of the Interior and SE “Infostruktūra”, the service provider for Secure State Data Communication Network (SSDCN)

The Ministry of Transport and Communications, the Information Policy Department of the Ministry of the Interior, and the Information Society Development Committee under the Government of Republic of Lithuania and the Communications Regulatory Authority (RRT) are working on the Network and Information Security (NIS) Law. A draft version is already available. It is planned to adopt the Law by the end of the year 2006. One of the objective of the NIS Law is the coordination of security policy and the raising of user awareness.

The Communications Regulatory Authority (RRT) together with the Ministry of Transport and Communications and the Information Policy Department of the Ministry of the Interior, are in the process of establishing CERT within RRT to coordinate activities of existing Lithuanian CERTs and ISPs on computer, network and information security incidents management. Establishment of CERT is foreseen by the end of the year 2006. One of the tasks of CERT will be the user education and awareness raising.

The Memorandum on the Progress in the Area of Security of Information and Networks was signed by the Communications Regulatory Authority of the Republic of Lithuania, the Association of Lithuanian Banks and the Association Infobalt (with 145 members of ICT sector) on 23rd November 2005. The Parties have agreed to set up a permanent Memorandum Implementation Committee (hereinafter referred to as the Committee), represented by authorized representatives of the Parties. The main tasks of the Committee are cooperation in the area of preparation and implementation of public awareness raising campaigns on the secure usage of the ICT and also cooperation to encourage the society to use security tools (antivirus and other software), that may protect from information and network security incidents.

By initiative of RRT, a TRANSITS *(Training of Network Security Incident Teams Staff)* training workshop for CSIRTs *(Computer Security Incidents Response Team)* was held on 29th-30th March 2006 in Vilnius, Lithuania. TERENA *(Trans-European Research and Education Networking Association)* and FIRST *(Forum of Incident Response and Security Teams)* in co-operation with ENISA organized this workshop. ENISA sponsored the event. The course dealt with the operational, organisational and legal aspects of incident response. It was aimed at professionals who are either members (or future members) of existing computer security teams, or who will be involved in building such a team within their organisation. 25 participants from 13 countries from the public and private sectors took part in this course: Lithuania (7), Estonia (3), Poland (1), Finland (2), Austria (1), Netherlands (2), Portugal (1), Germany (1), UK (2), Belarus (1), Azerbaijan (2), Kyrgyzstan (1) and even Afghanistan (1).

The first European network and information security conference *Readiness for Handling Network and Information Security Incidents* was held on 24th-25th November 2005 in Vilnius, Lithuania. The conference was jointly organized by ENISA, RTT and Ministry of Transport and Communications. The conference was attended by some 160 participants from all over Europe and gained a wide coverage in the media. The second European network and information security conference is planned for the November 2006 in Lithuania *Ensuring information and network security - a guide for managing security in public and business environments.* This year, ENISA, RRT, Ministry of Transport and Communications and the Ministry of the Interior will organize the conference.

Supporting material can be found at www.esaugumas.lt, www.vrm.lt (in Lithuanian only) and www.securityconference.rrt.lt.

National government as user of information systems

Recent awareness programmes and initiatives

The project “Strengthening capacities of authorities dealing with IT and Data Security” was implemented using PHARE funds in 2005.

According to this project, 15 experts working in IT security evaluation and consulting from different institutions were trained. More than 200 persons working in public institutions have been trained in the field of IT security using prepared training programme. (http://www.esaugumas.lt/VRM/VRM/index.html). Training programmes created by the project are available for State institution staff either in the form of compact disc or online on the web.

The Governmental strategy for electronic data security until 2008 intends to achieve the following objectives in the field of IT security awareness:

- Thorough education of public officials and employees working on employment contracts in electronic data security. The Ministry of the Interior is responsible for organizing seminars and preparation of training programme (including distant learning content). This is scheduled for Q2 of 2006 through Q4 of 2007
- The promotion of awareness regarding the importance of electronic data security. This responsibility lies with the Ministry of the Interior, the Ministry of Transport and Communications, Information Society Development Committee under the Government of Republic of Lithuania and the Communication Regulatory Authority. During the period Q2 of 2006 through Q4 of 2007 it is intended for the information regarding electronic data security and about the increasing number of information security breaches and threats to be produced in the form of compact disc and on the website http://www.esaugumas.lt. The Ministry of Education and Science, the Ministry of the Interior and the Communications Regulatory Authority intend to present new electronic data security training programs to secondary schools and universities. It is one of the main priorities that IT security awareness would be raised among school children and students (this category of people are the main users of Internet and other advanced technologies)

Government as partner with business and industry

Internet Service Providers (ISPs)

Meetings of national ISPs, market players and representatives of the Communications Regulatory Authority on NIS and the establishment of national CERT took place on May-July 2005 and are still going on in 2006.

Media

It should be noted that the examples listed below use media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

A survey to identify situation on NIS started in October 2005. Survey covered internet users, organisations and ISPs. Results: 78% of Internet users suffered from viruses, 63% from spam. 29% of organisations and 45% of ISPs had up-to-date NIS policy, 22% of organisations and 23% of ISPs didn’t have NIS policy. The survey with comments was widely covered by Media. Full report on survey can be downloaded following the link here (http://www.esaugumas.lt/get_file.php?file=RDovTmV3UlJUL3NhdWcvbS9tX2ZpbGVzL3dmaWxlcy9maWxlOC5wZGY7SW1vbmVzX0lQVF9hcGtsYXVzYS5wZGY7Ow==)

Also the TV and radio broadcastings were held on NIS issues with participation of representatives of RRT and other state institutions.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The new web site dedicated to awareness on NIS went live in February of 2006. The web site www.esaugumas.lt is dedicated for Internet users, SMEs and state institutions network administrators and is intended to be an interactive forum of NIS for all interested parties. Here articles, news, forum for discussions, advice on NIS issues, tools for users to avoid NIS incidents, etc. are available.

In cooperation with banks, RRT prepared a brochure to inform users about phishing and ways how to recognize those attacks and how to protect against them. 200.000 brochures were distributed over all Lithuanian regions.

RRT in cooperation with well-known security vendors worked together on the project “Safeguard your computer!” to produce a tool for home users, which will help to improve security on their personal computers. A CD Rom with the collection of necessary safeguard programs (antivirus, antispam, antispyware and others) and relevant information about secure use of internet has been developed. About 100.000 CDs were distributed free of charge through the Lithuanian regions in June 2006. The ending stage of the project was widely covered by Media.

Projects such as ”Safer Digital Lithuania” (raising awareness of users) and “Hotline Lithuania” (directed against harmful information on the internet) under the EU program “Safer internet” are ongoing. Partners for the projects are JSC “Bitė Lietuva”, Ministry of Education and Science, Information Society Development Committee under the Government of Republic of Lithuania, Communications Regulatory Authority and other public and governmental institutions. The timeframe of the projects are 2005 – 2007.

Government as partner with civil society

Recent awareness programmes and initiatives

Refer to the *Gov. as Partner (Business)* section for information.

18. Luxembourg

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Luxembourg have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as partner with civil society

Metrics and key performance indicators (KPIs)

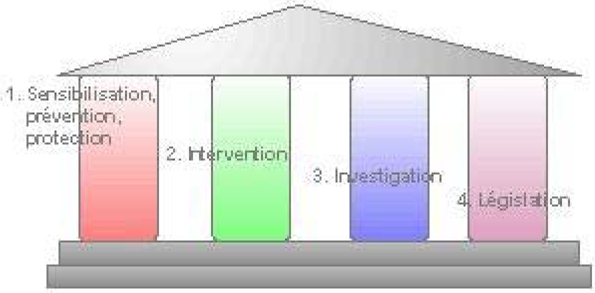
Lessons Learnt

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

Luxembourg has had a national strategy in the area of information security for several years. This strategy is based on four pillars which are:

1. Awareness raising and prevention
2. Intervention (CERT)
3. Investigation and repression
4. Legislation and standardization



Nature and scope of the strategy

The strategy is a national strategy, involving as many key actors as possible. Public and private sector are addressed in the strategy, both as sink and source.

Responsibilities

The government, specially the Ministry of the Economy and Foreign trade is coordinating the various projects. The responsibilities are with the different actors. The Luxembourg government has managed to bring many different actors together. They come from government, university, research institutes and industry. The coordination is done via a common platform. This platform discusses on the priorities, budgets and makes recommendations to the central government.

Objectives

The objective is to create consensus on the way how the strategy is deployed in the different areas and within the different communities of Luxembourg. It is important to know the different needs in order to invest the finite budgets on the most important projects in the different areas of the national security plan. It is also most important to be able to take advantage of synergies.

Target Sectors

The target sectors are very diverse, they cover the central government, industry, SME and of course citizens and children.

Actions identified

The actions that have been identified can be classified in the following areas:

- Awareness raising of citizens towards the risks of threats coming from the Internet like malicious software and attacks. The aim is to help citizens protect themselves correctly so that they can take advantage of the benefits of the Internet. They should use the e-government, e-health, services and take advantage of the advantages of e-commerce.
    - Basic knowledge of the threats
    - Implementation of basic security
    - Basic knowledge of risk analysis
    - Special focus on Bluetooth and WiFi
- Awareness raising of children on dangers of the Internet with specific children adapted content. They should be made aware of the existence of illicit and harmful content, the dangers of chat:
    - Harmful content
    - Chat
    - Basic knowledge of threats
    - Special focus on Bluetooth and WiFi
- Awareness raising of SME. The major goal is to make the SME aware of the true value of the different assets they have in their companies. Most SMEs are not conscious about the impact an incident could have. SMEs are also taught how to implement security. The concept of risks is introduced to them and they are also provided with material to write security policies (Risk analysis and policy deployment):
    - The concept of risk analysis
    - Assessment of resources
    - The concept of security policies (continuous amelioration)
    - Knowledge of threats
    - Knowledge of security implementation
- Awareness raising of industry mainly in the area of industrial espionage. Most Luxembourg companies are not aware of this threat. A large campaign is being prepared in this area. Targets are industry and banks:
    - Awareness of industry espionage
    - Awareness of social engineering risks
    - (technical security is well developed)

Timeframe and assignment of responsibilities

Citizens: actions all for this year. Responsibilities: Ministry of the Economy and Foreign Trade, Internet Café.

Children: actions all for this year. Responsibilities: Ministry of the Economy and Foreign Trade, Ministry of the Education, Youth service

SME: Ministry of the Economy and Foreign Trade, Professional Chambers, R&D projects co financed by EC.

Industry: Ministry of the Economy and Foreign Trade, State Ministry, Ministry, Police,

Web citations and/or relevant material

Citizens & SME: web site of CASES www.cases.lu. With detailed information on threats, warnings issued for critical vulnerabilities, flash guides how to configure correctly the WiFi-enabled ADSL routers sold in Luxembourg or how to recognize phishing attacks. Many hints and tips are available on the Internet site. The group is very proud of the guide on how to make a risk analysis and how to write an IT security policy. Special leaflets on different subjects are available.

Background information on: CSRRT-LU. Special designed early warning malware indicator on: CSRRT-LU. The last two resources are not designed for citizens and SME but give valuable information in order to inform this community correctly about threats.

Flyers and stickers are being developed

Children: www.mysecureit.lu; www.petitweb.lu, a project started by the TELINDUS and government: safer Internet and a special report being written about Internet security for children in Luxembourg. A large campaign made in all the schools together with the CLUSSIL and the Ministry of Education: Presentation

Industry: New project, only drafts on industrial espionage available. Special flyers on security and social engineering will be available soon.

Legal, regulatory, and institutional arrangements to raise awareness

The Luxembourg government has created a platform for information security hosted by a research institute. This platform brings together people from industry, R&D, government and research.

Luxembourg has legislation against cyber-crime in place. Luxembourg tries to stress more on certification than on regulation. The certificate e-commerce certified has been created to foster trust and confidence in e-commerce and to heighten security in e-commerce.

Luxembourg wants to make all stakeholders aware of their responsibilities and legislation is, as is believed, not the right approach; certification based on a broad consensus is quicker and more effective as it is a positive approach. It is also easier to ramp up security by changing certificate level than to adopt legislation, which is normally very slow.

National government as user of information systems

Recent awareness programmes and initiatives

The Ministry of the Economy and Foreign trade has launched a first project fully focussed on the security within ministries and administrations. During this project a risk analysis is being done in the Ministry and an information security policy is being written. The EBIOS methodology is used to do this risk analysis. The lessons learned during this project are forwarded to the other Ministries that want to launch this process.

Ne surfez jamais sans protection!
Protégez toutes vos connections
Êtes-vous une cible facile?
Pensez sécurité
Avant d'entamer le tour du monde pensez aux vaccins.
La protection antivirus
Vérifiez avant de consommer.
Malware
Cases.lu, les réponses que vous attendez aux questions essentielles que vous vous posez sur la sécurité de l'information.
CASES
www.cases.lu

The project will deliver awareness raising material specially designed for governmental employees. The results of the risk assessment have shown that the Ministry of The Economy and Foreign trade has a very high need of confidentiality. Special material will be developed for the issues of social engineering, and physical security, which are the main threats in the area of Luxembourg government. This material will be available under certain restrictions. In The Ministry the material will be provided via leaflets, posters and via the Intranet. Special courses will be given to people working in highly confidential areas.

The aim of this project is to implement higher security in the Ministry of the Economy and Foreign trade and to show other governmental institutions how to proceed in this area. Knowledge transfer is one of the major issues of the project.

The national IT department is performing a similar project in order to write a new IT security policy. This work is based on a different methodology: "BSI Grundschutzhandbuch" and the MEHARI method of the CLUSIF. Both projects are being done with the help of the CRP Henri Tudor and the University of Luxembourg. Knowledge transfer is considered to be most important in this area.

This double approach has been chosen in order to be able to compare the different methods in practice and to be able to elaborate a good practice approach for the central government. Luxembourg has; in the past few years they have acquired a high level of knowledge in the areas of risk analyses and security policies.

Local government as user of information systems

Recent awareness programmes and initiatives

Not started yet, only small projects are running, coordinated by the IT department of the Luxembourg communes. They wait for the lessons learned of the projects deployed in central government.

CRP Henri Tudor, University of Luxembourg and the project CASES will be charged to deploy the knowledge on local government level.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

Statistical information can be found on the Website of STATEC.

The main issue in SME awareness raising is to first of all to persuade SMEs to estimate the real value of the assets they have and they should protect. It has been learnt through many contacts with SMEs, that they completely underestimate the real value of their assets. They also underestimate the presence of threats, real threats. Industrial espionage exists on the smallest level; there have been cases where one shop is spying over the neighbour shop because of the prices and the customer database.

These messages learn about the real value of your assets, learn about the presence of threats, are the messages trying to be pushed forward to SMEs. This is done via the risk analysis and the guides that have been written in the area of the information security policy.

A clear understanding of the risk concept: RISK = vulnerability * threat * impact is a key issue. If SMEs understand this relation, they will be pushed by the reduction of impacts to reduce their vulnerabilities and build up countermeasures and preventive measures against threats. Indeed this is, as described by the OCDE document, a cultural problem.

Due to the fact of poor level of security existing in the area of WiFi, guides based on flash movies and on how to secure the WiFi-enabled ADSL-routers sold in Luxembourg have been produced. The percentage of the unsecured WiFi-routers deployed in Luxembourg is still very high.

For the moment the main channels used to forward information is still the web site, publication of articles in newspapers and workshops.

Unfortunately, no way to increase motivation of multipliers has been found. The know-how of the multipliers seems to still be very low and for this reason they do not dare pick up themes in the area of information security. It has also been seen that in media, vocabulary is often not correctly used; terms like hacker or cracker are mixed up.

Internet Service Providers (ISPs)

CASES has analysed the ADSL-routers sold by the Luxembourg ISPs. Strength and weaknesses of the routers have been published. Upon this publication, the central ISP (P&T) has changed one router because it was not secure enough.

The campaign shows people how to secure their router by correctly configuring the WAN (shut off of the not needed services) and how to correctly and safely set up the WiFi network.

CASES has also appealed to the ISPs during a national conference to work together with the national government to better inform customers upon how to secure their computers.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

CASES has not yet found a way how to convince media to pick up the theme of information security.

The project has however approached one of the most popular sites for young people in order to collaborate in the area of awareness raising. This has not yet led to a project, but the collaboration looks very promising.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Collaboration with the following private initiatives is running positively:

- www.petitweb.lu
- www.internetmonitor.lu
- www.mysecureit.lu
- www.party.lu

CASES has not yet started with PPPs with major vendors, because Luxembourg wants it's initiatives to stay independent.

A major campaign however is planned together with ISPs. CASES has created the basic content like the secure configuration of the ADSL routers sold in Luxembourg. This content will be the basis of a close collaboration between the project CASES and the ISP.

In the financial sector area, CASES is preparing collaboration with the ABBL (www.abbl.lu), the bankers association, in order to promote security certification ISO 27001. This cooperation is starting end of May 2006. Same approach has been chosen with industry.

PPP is increasing in importance, but CASES does not necessarily want to associate with security vendors, but with the communities that slowly start to see the advantages of an early awareness raising campaign. The initiatives in this area will surely increase.

Government as partner with civil society

Recent awareness programmes and initiatives

The project CASES fully covers the awareness raising campaigns targeted towards citizens (children and adults; no distraction to silver surfers). CASES organises conferences for adults in local communities and makes road shows on fairs.

Together with the Ministry of Education an awareness raising campaign for children has been organized. Every 13 year old child in Luxembourg is taking part in an awareness raising campaign organized in every school in Luxemburg. During these shows, children are made aware of the risks in information security (technical risks but also chat security). Information can be found in www.mysecureit.lu and on CASES.

CASES is also developing an e-learning portal for information security for citizens and SME. It is based on the huge content of the CASES site and should be publicly available as from end of 2006.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

KPIs have not yet been defined.

Lessons Learnt

It was found that most ADSL routers sold in the country were sold in an inadequate state (e.g. basic settings were not secure enough). Through collaboration with ISPs, this is now changing or has changed. Also, it has been important to cooperate with ISPs to increase reactivity for informing customers whose computer has been compromised.

19. Malta

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Malta have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The Ministry for Investment, Industry and Information Technology has drawn up a National ICT Strategy that runs from 2004 till 2006. The strategy includes a section dedicated to information security. This section of the strategy envisages a number of awareness raising initiatives targeting audiences from children to parents through to commercial entities. Among the objectives is the aim of raising awareness about the increasing number of information security breaches.

Refer to http://www.miti.gov.mt/site/page.aspx?pageid=4 for more information.

Furthermore, a National eSecurity Working Group (consisting of multiple stakeholders) was established earlier in 2006 with the key objective of developing and implementing a national Strategy and Action Plan specifically dedicated to eSecurity for the period 2006 – 2008. The strategy will include activities aimed at awareness raising covering all aspects of eSecurity – from network and information security to cybercrime through to data protection.

Legal, regulatory, and institutional arrangements to raise awareness

As detailed, a National eSecurity Working Group has been. Among others, the Terms of Reference for the strategic plan include the identification of, and making recommendations to address, any lacunae identified with respect to:

- the institutional structures, and administrative mechanisms necessary to address issues related to eSecurity in a holistic manner
- the required competencies within the public and private sectors to adequately address eSecurity matters

With regards to awareness raising, the working group is due to complete an ICT security review that will gauge the awareness of eSecurity among citizens and businesses and will recommend measures the can be taken in order to minimize risk at the various levels.

National government as user of information systems

Recent awareness programmes and initiatives

Following the establishment of various eGovernment Services, the Ministry for Industry, Investment and Information Technology (MIIIT) has launched the eID project. Through this electronic identity card, the user will be able to access all electronic services offered by Government in a secure manner.

Local government as user of information systems

Recent awareness programmes and initiatives

The programmes organized so far have mainly been carried out by central government. One should note however, that the small size of the country makes national awareness campaigns more feasible than may be the case in larger nations.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

One of the most influential initiatives in this regard is expected to be the Micro-Enterprise Acceleration Programme (MAP) which led to the establishment of a training course on how enterprises can use ICT in order to improve the success of their businesses. The initiative is being coordinated between MIIIT and HP, a leading organisation in the ICT field and should be launched in the coming months.

The primary goal of this course is to demonstrate how micro-entrepreneurs can improve the success of their businesses using ICTs. To achieve this goal, the Smart Technology for a Smarter Business™ curriculum focuses on helping micro-entrepreneurs do the following:

- Gain awareness and comfort with ICT
- Gain knowledge and skills in the business applications of ICT
- Use ICT to improve their business' efficiency and growth.

A secondary goal of this course is to provide participants with the opportunity to assess their needs for further training and technology investment. Finally, this course offers participants the opportunity to share their ideas, experiences, and advice with each other. Learning from the varied business experiences of other participants is an important component of this course.

In addition, in order to enhance the ICT skills amongst employed people, the Government has embarked on the MyWeb Corporate programme. The Ministry facilitated the distribution of basic ICT skills courses to employees in a number of enterprises that have shown interest in the course.

In this case, participants are being trained on the basic use of personal computers and the Internet. The course includes a module dedicated to Internet Safety in order to raise awareness of the threats that may be encountered in the online world.

MIIIT is working on another initiative which is to oversee the establishment of a local trustmark label. The label is expected to encourage businesses to implement security measures to their online systems, whilst serving to increase trust in eCommerce.

Internet Service Providers (ISPs)

MIIIT and a leading Internet Service Provider in Malta have embarked on a joint awareness raising campaign for children. The campaign will target year 1 students who will be introduced to the virtual world, and at such an early stage, be taught the do's and don'ts of the Internet and what the issues that they should tackle with caution are. The initiative is being sponsored by the ISP in question whilst MIIIT is providing the required human resources, expertise, and is facilitating the organisation of such events in schools and other institutions.

In addition, the Ministry is seeking to cooperate with various public and private entities to embark on an intensive awareness campaign. It is expected that a proposal for funding under the Safer Internet Plus programme will be submitted. The campaign will target children and parents and will focus on security issues related to services delivered over mobile phones.

Media

It should be noted that the examples listed below use media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

The latest awareness raising initiative that the Ministry has embarked on was launched in February 2006. The month-long campaign was a joint effort between MIIIT, Maltacom and Microsoft.

The campaign aimed at creating awareness on how to provide a safer Internet environment for children by informing parents and guardians without causing any unnecessary alarm.

The campaign was based on the results that were obtained through a National Survey. The survey outlined the major threats and difficulties that children are encountering in the online world. These difficulties were kept in consideration when planning the campaign in order to provide solutions to these 'problems' and transmit the right message to parents and also to the children.

The campaign made use of television and newspaper adverts, television and radio interventions and also the distribution of leaflets and other material to students in both public and private schools.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Once of the most effective PPPs was the joint effort between MIIIT and Microsoft. This led to an intensive awareness campaign that targeted children and parents on the safe use of the Internet. This initiative has given the Ministry the opportunity to raise awareness about the latest security threats and provide solutions on how these threats could be overcome. A section on the Ministry’s website was also created (www.miti.gov.mt) which is regularly updated and provides a variety of useful information to both parents and children.

In addition, the Ministry has signed an agreement with Childnet International, a UK based non-profit organisation which has given the Government the permission to make use of various Childnet resources and materials which were prepared by experts in the field of Child Safety over the Internet. This has facilitated the delivery of presentations and seminars which have provided parents with information on how to protect children from security risks encountered when using information technology.

Also refer to the previous text for initiatives with ISPs for more information on public-private partnerships.

Future public-private partnerships

MIIT is currently in discussion with Childnet International with a view to reach a second agreement with organisation. The agreement will be a follow up to the first, and will provide the Government with more up-to-date information on the latest threats that IT users are experiencing. This is expected to be extremely useful in future awareness raising activities that the Ministry will be embarking on.

Government as partner with civil society

Recent awareness programmes and initiatives

MIIIT (for the past 3 years), has been organizing regular courses in basic ICT literacy for the general public (parents, children, elderly etc). The Ministry has recently revised the course curriculum to include a module that tackles Internet Safety and the do’s and don’ts of the Internet. This module will give the attendees the necessary information on what they should be aware of and how to tackle the problems that they might encounter in the online world.

MIIIT has also cooperated with various organisations involved in the ICT field, to issue a nationwide survey amongst children and parents. The survey is aimed at obtaining information on how children are making use of the Internet and their parents’ perceptions in this regard. The results obtained were used in planning and proposing new initiatives on the subject.

MIIIT is also planning to launch a periodic Information Society Review that will tackle particular areas of interest/importance. The aim of the publication will be to give people a picture of developments regarding ICT. The first edition of the Information Society Review will be dedicated to eSecurity. The objective will be to outline the issues commonly encountered and propose measures that could be adopted to ensure safe use of ICTs.

Children are regarded as the most vulnerable to the threats that IT could present. In view of this, MIIIT has recently embarked on an intensive awareness campaign targeting parents and children aimed at raising awareness of these threats and recommending solutions to make protection easier for all. The campaign was a joint effort between MIIIT and Microsoft, the latter providing the funding for the campaign, whilst the former provided the local expertise and human resources.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Also refer to the previous text for Public-Private partnership initiatives in the *Gov. as Partner (Business)* section for more information on PPPs.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

At this stage, the Ministry does not use metrics or KPIs, however, the Government plans to develop such metrics as it proceeds within the set programme on Internet security and safety.

Importance of Metrics/KPIs

This importance of metrics and KPIs is recognised and accepted. Such figures will help the Government plan upcoming initiatives better and serve as a guide for future projects.

20. Netherlands

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Netherlands have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

In October 2001 the Dutch government initiated the national awareness campaign SurfopSafe (which translated is “Surf on Safe”). This campaign was combined in June 2003 with the European SafeBorders awareness project and became the Dutch Awareness Node NaNSoS in November 2004. From 2002 until 2005 the Dutch Government facilitated the KWINT programme, a national public-private partnership programme on Internet vulnerability, coordinated by ECP.NL. KWINT also had a strong awareness raising theme.

In October 2005 the Dutch Government boosted efforts in awareness raising campaigns by reserving money for three years (starting 2006) and asking ECP.NL to be the co-ordinator for the campaign, while at the same time asking the current National Awareness Node to join forces with ECP.NL. This has resulted in the national Digibewust campaign. This means the SurfopSafe campaign (and thus the current awareness node) is to be combined with campaigns initiated by private parties such as Microsoft and KPN Internet to ensure maximum synergy and optimal results.

Nature and scope of the strategy

- Assignment of responsibility: the Ministry of Economic Affaires has ordered ECP.NL to develop the Digibewust Programme and to facilitate the roll out
- Objectives: develop a framework in which the target sectors can act in a public-private partnership on awareness raising for secure electronic communications
- Target groups: Home user (young, female and silver surfers), SME and industry. The Awareness Node is included
- Timeframe: 2006-2008. ECP.NL is working with strong indicators. Individual projects must be market driven and have measurable targets which will be evaluated afterwards
- Assessing the impact of the strategy: the programme must be effective, with measurable results and supported by a broad cooperation of national stakeholders. Every year a questionnaire will be addressed to stakeholders where they can fill in a total score to the programme. The objective is an average score of 7.5. The brand awareness of the campaign should increase 25% a year for every target group

For more information, visit www.digibewust.nl

Legal, regulatory, and institutional arrangements to raise awareness

There does not seem to be any legal, regulatory or institutional arrangements for awareness raising in the Netherlands. The aim is for self regulation and public-private partnerships.

Legal, regulatory and institutional arrangements

- Promotion of security for public and private governance: the Digibewust Programme will organize a national event to share knowledge and best practices twice a year. All kinds of security themes and topics will be discussed including science, SMEs, industry and government
- Promotion of best practices: the several platforms for industry (vital infrastructures, education, certification and security R&D) are also discussing best practices
- Information and education campaigns:
  - A website (in Dutch), www.digibewust.nl, is the basis for several hundred pages of Internet-safety related information focused on individual target groups (children, parents, educators, SME). The site contains or will contain several on-line tests, a port-scan, case studies, course materials, etc.
  - A website (in Dutch) www.ecp.nl, provides information on a wide range of security-related subjects. Moreover, a biweekly newsletter is issued which reaches thousands of users
- International co-operation: all national security platforms are aware of the international developments. ENISA can play an important role in this

The 'old' SoS and KWINT publications or initiatives are being used again:

- Various awareness materials (such as brochures and leaflets) have been developed aimed at various target groups. Examples vary from a phishing flyer (where the Dutch consumer organisation distributed 800,000 copies) through to a leaflet sent to all Dutch high schools on netiquette
- A code-of-conduct was signed by the major Dutch chat rooms for safeguarding minors. This was initiated and co-ordinated by ECP.NL.
- Various activities have been undertaken or are underway relating to the European Insafe network. One example was the organisation of a story-telling contest - the winner of the award will be present at the European award ceremony in Paris in December
- The organisation and attendance of various national events. These include several stakeholder meetings relating to Internet security (March 2005 by NaNSoS and October 2005 by ECP.NL), a stand at the largest Dutch educational fair in February 2005 and a stand at the largest Dutch ICT related fair in November 2005
- The celebration of the second European Safer Internet Day on 8th February 2005 and the organisation of the third one on 7th February 2006. On this day, NaNSoS will start a month-long campaign where children and youngsters will be encouraged to tell their teachers, parents/grandparents and other grown-ups what they are doing on the

Internet and what the associated risks will be. This campaign will be supported by the public-private partnerships ECP.NL is organizing. This will result (amongst others) in the joint launch of a campaign started by Microsoft, KPN and others on Internet safety

National government as user of information systems

Recent awareness programmes and initiatives

ICTU[13]

The ICTU-foundation was established on 11th April 2001 by the Ministry of Home and Kingdom Affairs. The motto of ICTU: helping government achieve better results with Information and Computer Technology (ICT). ICTU combines knowledge and experience in the field of ICT and government. ICTU carries out various programs for and in cooperation with governmental organisations. Policy is translated into specific projects for government. In the board of ICTU all layers of government participate: state government, provinces, local communities and district water boards.

[13] Text quoted from: http://www.ictu.nl/profile.html

Local government as user of information systems

Recent awareness programmes and initiatives

eGEM[14]

EGEM supports councils in improving their service and their way of processing by effective and efficient use of ICT. This is not confined to development of various products and services, such as standards and models of reference.

EGEM has an eye for things already developed by councils and has undertaken the task of spreading the existing knowledge: “Crib, imitate, EGEMulate’’. Local councils which would like support for specific issues at implementing e-government projects can use EGEM-i (the ‘i’ stands for implementation or introduction).

[14] Text quoted from: http://www.ictu.nl/profile.html

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

Since 2000, Syntens executes the SME part of the programme “Nederland gaat digitaal”. Data protection is one of the themes within this ebusiness programme. The emphasis has switched from the importance of good Internet sites for entrepreneurs applying the use of the Internet in several organisational processes, to a broader coverage in the application of new possibilities with ICT. First the focus laid on micro-enterprises, now small and medium enterprises are addressed.

Syntens actively aims at the micro-enterprises with more than five employees (ca. 60,000 ventures) and the small and medium enterprises (ca. 64,000 ventures). The focus lies within the following sectors: producing industry, food and agriculture, logistics and wholesale, creative industry, ICT, multimedia, construction and human health.

In 2005, around 350 workshops (with 5-15 entrepreneurs) were organized by Syntens. Twenty of those focused on data protection, specifically aimed on the Internet. These workshops occasionally result in individual recommendations on data protection. There were hardly any requests for advice or knowledge within the theme of data protection.

As part of the programme, entrepreneurs could fill in an online questionnaire through which they could get a first impression of their own situation. It was support with the booklet "With a safe feeling, data protection in practice". Specific figures on the consultation of the booklet and online questionnaire are not known. The booklet is still available, but the online questionnaire is no longer actively used. Currently, a new scan is available online that puts the emphasis on the introduction of making payments through the Internet, as part of the companywide method 'ready for digital business'.

The level of technical aptitude is low. It is especially aimed at the entrepreneur. In practice, it shows that for small and medium enterprises the person responsible for marketing and/or sales participates. Workshop leaders are mainly Syntens advisors with an affinity for ICT; the workshop programme is defined centrally and set up by an external expert party.

Experience shows that the attention increases in a period with many virus outbursts and a lot of media attention. Participants like to hear that the problem is not that substantial and that they do not have to invest in various measures. There is much interest in free virus scanners, practical advice on the settings of their computers and software, and standard agreements with a website builder or host.

A new activity underway is measuring the current state of experiences with cyber crime, awareness and actual data protection within a group of fifty organisations on an industrial estate, chosen randomly. For this, a questionnaire, interview, workshop and a demonstrator are used; repairing services are offered by the ICT 'house supplier'. The results will be extrapolated to the Dutch MKB (October 2006) and will lead to a project proposal.

NPAC

In the Digibewust programme an experiment amongst fifty small and medium enterprises starts at the end of April 2006 to increase the insight in the vulnerability of cybercirme attacks within SMEs.

This experiment aims to identify reasons or answers behind questions such as “do they experience cybercrime as a problem” and “are their computers sufficiently protected”. The results of the measurements will be used as a starting point in further activities. The end goal of these activities is to reduce the damage done by cybercrime as much as possible.

Internet Service Providers (ISPs)

There does not seem to be any cooperation between ISPs and the government with the exception of the Dutch hotline. The branch of industry NLIP does not exist anymore and without support from the government, the hotline for illegal content is not operational.

The following links detail the surveys of the Ministry of Economic Affairs and other surveys conducted on the Internet market: http://www.onderzoeksdatabank.minez.nl/onderzoeken/onderzoekskaart.aspx?onderzoekID=2934 and http://www.onderzoeksdatabank.minez.nl/rapporten/Rapport.aspx?rapportId=485

For details on an awareness campaign supported by the Dutch Hotline, refer to www.surfsafe.nl

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Also refer to the text for Public-Private partnership initiatives in the *Gov. as Partner (Society)* section for more information on PPPs.

Government as partner with civil society

Recent awareness programmes and initiatives

The Dutch Consumer Organisation operates independent of civil bodies.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The massive use of the Internet and new online technologies has brought the Netherlands its share of online problems. These tend to be similar to those in other countries with relatively high Internet literacy, being computer viruses, spam, unwanted contacts (e.g. chatrooms or online bullying), online fraud and identity theft, hacking and inappropriate content. The number of incidents reaching prominent press coverage has increased in the last year and this has led to more and more requests for information from schools, parents and politicians. To counter these threats, the Netherlands Ministry of Economic Affairs has in 2005 decided to intensify the existing awareness campaign SurfopSafe and align it with other activities, both from the government itself as well as those from private parties. This program (Digibewust), which will run for three years starting 2006 and will be co-ordinated by ECP.NL, is aimed at educating and empowering end users, ranging from children to general consumers and SMEs. Its goal is to make them not only realize and understand the issues, but also to act accordingly to minimize the existing threats. This is a step forward from the existing Dutch approach.

Currently in the Netherlands the main issues related to Internet safety are:

- Education of children, teachers and parents on the potential risks of the Internet. This follows several incidents involving youngsters and either paedophiles, online bullying or unwanted online experiences. Several initiatives have been launched to reach children, teachers and parents, among which are a code of conduct for chat rooms (co-ordinated by ECP.NL), sites for parents and teachers (by the major Dutch Internet provider KPN Internet) and the activities of the current Dutch Awareness Node NaNSoS. These include sending information materials to all Dutch schools, being present at the main Dutch educational fair, and organizing the Safer Internet day 2006 (with the theme "Let children teach the grown-ups about Internet safety!"). Moreover, NaNSoS is active in promoting the Dutch Internet Certificate (developed under the label of the Awareness Node by the Ministry of Economic Affairs), for primary schools and officially launched in October 2005. The approach taken is not one of "ban and control", but rather one of "educate and instill responsibility"

- Organized computer crime, such as phishing and identity theft. Several rather amateuristic cases have been reported in The Netherlands recently, but it is expected that this threat will increase and that more professional cases will show up. Also the use of botnets (e.g. for fraud and extortion) are beginning to be a more serious threat, demonstrated by the recent police raid on three young men who were 'owners' of a botnet of over one million zombie computers

Since 2001, when the Dutch National Government Awareness Campaign SurfopSafe started, a large number of bodies in The Netherlands have adopted the issue of safer use of the Internet. Among these there are major Internet providers (who now use Internet safety as a marketing tool), the Dutch consumer organisation and several foundations (such as the NICAM, the Safe Internet Foundation, Bits of Freedom, the children's consumer organisation). Moreover, the government has sponsored ECP.NL to carry out a program on Internet safety, installed an Internet security incidents early warning service (www.waarschuwingsdienst.nl, related to the government CERT organisation) and launched the safer Internet certificate for primary schools. The details of this government awareness campaign are given below.

In September 2005 the results of a large governmental study to measure the state of awareness related to Internet safety in The Netherlands were published. The general conclusion of the research is that, while basic awareness of the dangers associated with Internet use is relatively high, only a limited number of people take appropriate measures. Moreover, there seems to be a rather high level of acceptance of Internet-related problems. These can range from loss of money to embarrassing situations with private photos being spread around the Internet. For children, it has become clear that there is a large gap in knowledge between children and their surrounding environment, such as parents and teachers. This was confirmed by several other studies (e.g. an effort carried out by Planet Internet, the largest Dutch Internet provider). All studies indicate the need for more focused awareness raising where the separate target groups are provided with specific awareness tools aimed at them. Moreover, a step should be made in getting people to not only be aware of the issues, but act on them as well.

Results

The first tangible result of the national Digibewust campaign was the joint celebration of Safer Internet Day 2006, where the National Awareness Node organized a number of activities, as well as private parties such as Microsoft, UPC, KPN, ANWB, TPG, IBM. Several public bodies /NGO's also organized the activities including the Dutch Consumer organisation, Govcert, and ICTU; a massive multimedia campaign was launched which will actively take part in promoting and organizing activities.

The role of the proposed awareness node

The proposed awareness node will continue the work performed under the current NaNSoS awareness campaign. To ensure an even stronger presence in The Netherlands it will, however, be merged with the public-private partnerships ECP.NL is organizing on Internet safety in Digibewust. This is supported by both the Dutch government, major industries as well as public organisations such as NICAM (of Kijkwijzer-fame) and Kennisnet.

The node will closely co-operate with all relevant national parties and especially with the Dutch government, the intended co-sponsor of the awareness node. Moreover, co-operation with other European countries will be actively pursued.

While not all actions can be foreseen at this stage, several concrete actions have already started under the current projects or are in the conception phase. Selections of these activities include:

- The promotion of the "Internet Safety Certificate" for children in the last years of primary school
- A Children's Board (DigiRaad) to advise on issues or questions
- Quest
- Campaign on passwords
- Involvement of child care organisations in the Dutch awareness campaign
- Closer involvement of SMEs with the campaign. This target group is often neglected and is currently suffering severely from issues related to Internet safety.
- The annual celebration of the Safer Internet day, where every year a new theme is chosen

The awareness node project will establish the Dutch campaign as a long lasting one and will investigate the possibility to have the node adopted (e.g. by a Steering Committee, combining several organisations active in the field of safer Internet use).

21. Norway

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Norway have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

Government as partner with business and industry

Government as partner with civil society

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The Norwegian strategy builds on the 2002 OECD document "Guidelines for the security of information systems and networks". The strategy has introduced the concept of a "culture of security" relating to IT and Internet usage, built around the development and deployment of information systems and electronic information exchange in Norway. IT security shall be one of the key factor's governing IT use by Norwegian businesses and consumers.

Nature and scope of the strategy

- Assignment of responsibility: Government and regulatory bodies
- Objectives: potential threats, options, limitations and necessary actions to advance establishment of a culture of IT security
- Target groups: the strategy stresses that all participants shall be made aware of information security; at present however the focus is on raising consciousness with SMEs and households
- Timeframe: Ongoing activity

Refer to www.norsis.no and www.nettvett.no for more information.

Legal, regulatory, and institutional arrangements to raise awareness

In 2004, the Co-ordination Body for information security was formed (led by the Ministry of Government Administration and Reform). It draws members from ministries and agencies that have formal responsibilities with regard to regulations as well as operational roles in following up on information security matters in a broader sense. Norway saw the creation of this body as a necessity due to the increased use of ICT which can also increase the risk for "attacks" and sabotage of IT systems. Its work covers general and overarching ICT-security questions connected to the security of the country, such as crucial national security interests and critical society functions. The organisation will co-ordinate the forthcoming work on ICT-security legislation, create common standards, norms, methods, and tools for ICT-security as well as coordination of security monitoring practices. It should also point out current issues and vulnerabilities of security risks and co-ordinate security information initiatives and readiness planning.

The Norwegian Centre for Information Security (NorSIS) was formally established on the 1st January 2006. The main activities consist of:

- spreading information, expertise and knowledge about possible threats and relevant countermeasures
- establishing contact and cooperation with organisations providing similar services in other countries

The Norwegian Post and Telecommunications Authority (NPT) is the regulator of the electronic communications sector. The regulator is responsible for enforcing the act on electronic communications which contains several provisions related to information security. The NPT is currently emphasizing its initiatives related to promoting security.

Norway has arranged a “Safer Internet Day” twice (in 2005 and 2006). It is planned to make this an annual event.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

There are currently no awareness raising initiatives aimed with or in cooperation with SMEs apart from that mentioned below.

Internet Service Providers (ISPs)

The most recent and successful government national initiative at raising awareness among users has been establishing the website www.nettvett.no, which has information on how to use the Internet and related services. The website was launched on the 26th April 2005 and was a collaborative project between several government entities and ICT businesses including ISPs. The responsibility of establishing the website was with the Norwegian regulator e.g. the Norwegian Post and Telecommunication Authority (NPT), which is also responsible for maintaining the website.

The website provides information, advice and guidance for secure and safe use of information and communication technology when using the Internet and Internet applications. As it is an awareness raising initiative, the aim is to contribute to increased knowledge among the general population and SMEs within the field of information security. Some of the themes covered include:

- Secure connection to the Internet
- Secure and safe use of e-mail
- Spam
- Phishing
- Protection against loss of data
- Confidentiality issues
- Protection against attacks from the Internet
- Securing a wireless network
- Use of digital signatures

The information on the website is presented in a logical manner with the themes divided into several categories. The information is also categorized into knowledge levels such as “for beginners”, “more advanced users” and “for businesses”. For most of the categories or themes, the website also gives short and easy to remember rules for what to be aware of when using the different Internet applications. The user can also post questions to the website if they have questions related to the content on the website or on related themes.

The site was launched on a specific day marking ICT-technology with a press release and an arrangement where the press was invited. National press was used as the main communication channel in relation to the launch was. Other events such as the national Safer Internet day on the 7th February 2006 have been used to promote the website. To try to get an idea of how successful the site has been, the number of unique hits has been counted. Currently the usage of the website is increasing and is now at about 1000 unique users per day. To be able to get a better idea on how satisfied the users of the website are, there are plans to conduct an online survey compromising of a simple set of questions that will pop up.

The website has recently been supplemented with animation (explaining viruses and firewalls) and most recently has been supplemented with an interactive game/quiz where users can test their knowledge level in IT-security. It is hoped that the quiz will stimulate the users to be interested in knowing more about the website themes. The future plan for the website is for it to become one of the leading national governmental websites that provide the public and SMEs with the most up-to-date information, advice and guidance within the field of information security.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

In relation to the “Safer Internet Day” in February 2006, several ministries, regulatory bodies and some larger private ICT companies co-operated with the writing (and financing) of a special insert (24 pages) in one of Norway’s largest newspapers. Beside this initiative there has not been any joint action with the Media.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

The NorSIS working expenses is funded through a PPP between the Ministry of Government Administration and Reform and a local knowledge-based company.

Government as partner with civil society

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Refer to the *Gov. as Partner (Business)* section for information on initiatives targeting citizens.

22. Poland

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Poland have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with civil society

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

In the area of consumer protection, the President of the Office for Competition and Consumer Protection bases the scope of activities on the government document “National Consumer Protection Strategy for Years 2004-2006”. One of the aims of the Strategy is to build a consumer friendly market. This aim should be achieved by monitoring electronic commerce and through pro-active education and promotion.

Legal, regulatory, and institutional arrangements to raise awareness

One of the significant examples of the cooperation within the central government administration authorities against spam is the Polish Spam Task Force. It is an important example of the horizontal co-operation among central administration bodies. The co-operation was established by the decision of the European Committee of the Ministers Council in autumn 2005. A “Coordinator” or “Contact point” was established on a national and international level whereas in other authorities (such as the President of the Office for Electronic Media Communication, the President of the Office for the Competition and Consumer Protection and the General Inspector for Data Protection), nominees were selected as national “Competent Authorities”. All of the mentioned authorities co-operate and investigate together, but each of the authorities has the domain over its competences. An important element in any decision is public-private sector co-operation. The Minister of Transport and Construction was obliged to undersign a contract with the NASK institute for technical assistance and support in Internet investigations.

National government as user of information systems

Recent awareness programmes and initiatives

The National Computerization Plan (the NCP) for 2006[15] details the level of development of eGovernment and is a starting point for discussion on the priorities for the computerization plan for the years 2007-2010. The NCP derives from the Act of 17th February 2005 on the Computerisation of Activities of Entities Performing Public Tasks.

The NCP is an instrument used to plan and coordinate computerization activities of public bodies with regard to tasks being fulfilled by these bodies. In 2006 activities within the NCP will focus on elaborating on the assumptions for changes in legal acts to ensure conditions for effective modernisation of ICT based public administration. This includes: looking at the restructuring of the processes; devising methods for coordination and monitoring of main eGovernment projects; developing a National Interoperability Framework for ensuring effective provision of electronic public services. The NCP has set two priorities for computerization in 2006 and subsequent years: streamlining public expenditure for IT projects within public administration and the creation of a modern and citizen-friendly state.

In area of security, the NCP's priority is in raising trust within the business environment and society when using electronic means to conduct public services. This is to be done firstly by introducing a consistent security policy within public administration. The following targets have been set:

- ensuring appropriate levels of security for public administration IT system – this is indispensable for creating trust within the users
- the popularization of electronic forms of identification - with respect to regulation of protection of personal data
- combating spam and other malicious occurrences causing threat to IT systems, including all illicit actions
- creating conditions for the increase of awareness and education of users with regards to protection of their systems against malicious software and spam – this includes notifying the appropriate body of the threats encountered.

It should be mentioned that, on the contrary to previous strategic documents, the NCP is being established by means of regulation and is presumed to have a stronger implementation effect than former strategies.

[15] National Computerisation Plan for 2006 (draft), Bulletin of Public Information, Ministry of Interior and Administration. The NCP is to be adopted by the Council of Ministers in May 2006.

According to *i2010 – European information society for growth and jobs*, each of the Member States should elaborate their own security action plan. This suggestion might be looked at in the forthcoming NCP for the years 2007-2010.

In March 2006 The President of the Office of Competition and Consumer Protection (OCCP) participated in an ICPEN project called *Fraud Prevention Month*. The project was devoted to "legal, economic and social aspects of unsolicited communication or spam".

The entire project had been developed together with business sector partners. Moreover, the OCCP has invited other public authorities responsible for consumer protection in Poland. As a result, in March 2006 the President of the OCCP in co-operation with business partners organized three extensive events.

- The first event was prepared together with the Polish Chamber of Information Technology and Telecommunications (PIIT). The President of the OCCP and PIIT invited the leading Polish ISPs and telecommunication operators. The target of the project was to discuss potential areas of co-operation between administrations and ISPs and the possibility of creating an anti-spam code of conduct
- The second project was a conference organized together with the NASK institute (the Research an Academic Network organisation controlled by the Polish administration and the leading Polish network operator). The OCCP and NASK invited delegates from academia, business and administration circles and initiated a dialogue concerning the possibility and necessity of introducing changes in the Polish legal system on spam enforcement. The OCCP and NASK also presented the guests with ICPEN initiatives such as the London Action Plan, Internet Sweep Day, Spam Zombie and other international projects such as the OECD Spam Toolkit (Spam Task Force) and the CNSA cooperation procedure
- The last significant event held by the OCCP was a workshop for public prosecutors on leading investigations on the Internet. The workshop has been prepared together with NASK and the leading Polish ISPs (Interia.pl and Onet.pl), as well as with the prominent Polish Internet auction house, Allegro

In March 2006 the OCCP experts on spam gave numerous press, radio and TV interviews. They reached various media including daily newspapers, local newspapers, branch Internet portals and popular women magazines.

Local government as user of information systems

Recent awareness programmes and initiatives

In the area of awareness programs derived by local government entities, the following initiatives can be highlighted:

- Initiative on awareness raising set up by the Association of Polish Districts and three leaders on IT technology in the Polish market (Symantec, Microsoft and Polkomtel). The Association of Polish Districts, founded in February 1999, has members in 313 districts The district cities have organized a series of seminars and training sessions in 2005 and 2006 based on awareness raising. More information on www.zpp.pl (in Polish only)
- Initiative on awareness raining set up by the e-administration club, which associates self-government and government organisations. Established in October 2003, the mission is to gather and exchange knowledge on implementation of IT technology in administration. E-administration club has organized and co-organized with other organisations several training courses on IT technology. Twice a year, the E-administration club organizes a conference called “Forum of IT in e-administration”. This year the VIth Forum of IT in e-administration was held in Toruń (Poland) on 25th and 26th April. Awareness raising on ICT was an important point at the conferences. The E-administration club has also organized special conferences on awareness raising; these include a seminar held in September 2004 on the auditing of IT systems in administration as a requirement of law and basis for quality certification on IT security, and a workshop on awareness of information security which was planed for 23rd May 2006. The main topics of the workshop was: the objective worth of possessive information; most important acts and standards concerning managing documents; information security policy as a basic element of IT systems; information threat prevention on PC workstation and mobile devices; methods and techniques for document authentication; socio-technical attacks and how to prevent it. For details refer to: http://www.e-administracja.org.pl/konferencje/2006/sbi3/index.php

Government as partner with civil society

Recent awareness programmes and initiatives

Since 2005, two projects have been underway in Poland as part of the European Commission's *Safer Internet Action Plan*. Both projects are under the auspices of the Ministry of Education and Science, the Interior and Administration Ministry, the Children's Ombudsman, the Police Headquarters, the Office for Competition and Consumer Protection, and UNESCO.

The first project is NIFC Hotline Polska (http://hotline.org.pl/). This project is managed by the Dyżurnet team of NASK (the *Research and Academic Computer Network*). The project objectives are organizing and maintaining a Hotline that receives reports on illegal content published on the Internet. The Hotline cooperates with the police in tracking down offenders who post illegal content on the Net and eliminates such content in cooperation with the respective ISPs. The Polish NIFC Hotline—Dyżurnet.pl team became a member of the INHOPE Association on the 28th January 2005, and received full membership within a year. In March 2005, a Consultation Committee was established by Dyżurnet.pl to help create better conditions in Poland to develop a culture of safety on the Internet. Many public authorities, ministries and organisations are involved in discussions in the framework of the Consultation Committee.

The other project is maintained by the Awareness consortium formed by NASK and the Nobody's Children Foundation. The proposal to establish the “Awareness” Node was submitted in response to the European Commission's *Call for Proposals 2003/2004* and is also based on the European Union guidelines presented in the *Safer Internet Action Plan, Work Programme 2003-2004*. In December 2004, NASK together with the Nobody's Children Foundation signed an agreement and became partners of the INSAFE consortium managed by European Schoolnet, which coordinates the work of national “Awareness” Nodes at the European level, on behalf of the European Commission. The Awareness project aims at creating a centre that would raise awareness of threats that the youngest users in Poland face on the Internet. The project has been underway since January 2005. The project involves training sessions for different targets including those in the education sector, Internet service providers, prosecutors and police officers involved in combating cyber crime. Conferences organized in 16 large cities promote safe content with an aim to help reduce the scale of threats that could come from the Web. A national pro bono media campaign is also planned for 2006. Awareness Node has also run the idea of the National Coalition for Safer Internet in executing an initiative where everybody can participate starting from www.saferInternet.pl web site. Participation in the “Awareness” project also involves cooperation with institutions that work to ensure safe Internet use. The consortium has recently been invited to preparatory negotiations for input/work with another *Safer Internet* programme that will be implemented in the years 2007/2008. The project is co-sponsored by NASK and the Nobody's Children Foundation, with 50% co-sponsored by the European Union.

Previously in 2004 the Foundation started the program “Dziecko w Sieci” (Kid on the Web) which is focused on raising awareness in children of the threats coming from Internet. Refer to www.dzieckowsieci.pl (in Polish only).

Another initiative that NASK has carried out for many years under the auspices of the Minister of Science and Information Society Technologies (now the Minister of Education and Science), is a series of “SECURE” annual conferences that promote the awareness of network and computer system security. The conference date back to 1997 and are considered to be the most respected such events in Poland. The organizers are NASK, the CERT Polska response team, and since 2005, ENISA. During the conference opening ceremony, a Ministry representative usually delivers an inaugural lecture on topics that include the public sector’s involvement in developing eGovernment in Poland.

NASK and CERT Polska also maintain a very important website in awareness raining for IT Specialists and Home Users; information on the website include details on new threats, vulnerabilities, incidents and preventive information as well as warning on possible attacks. Refer to http://www.cert.pl/

23. Portugal

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Portugal have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The coordination of the strategy for information security is the responsibility of UMIC (Knowledge Society Agency, www.umic.pt). The overall objective is to define a National Information Security Policy.

UMIC has published a document that has a wide set of strategic objectives related to the creation of a culture of information and network security in the key sectors of the Portuguese society. Due to the nature of the information society and the responsibility of the Government, the strategy is more directed to the public sector.

Several activities are already being implemented by the government and other public and private institutions under the mandate and supervision of the government.

Legal, regulatory, and institutional arrangements to raise awareness

There are no legal or regulatory measures undertaken for the specific case of awareness raising. However several initiatives have already been implemented, such as:

- The creation of the Portuguese CERT (www.cert.pt). Initially created for the research and education sector, activities have now been extended beyond this set of users
- Training courses have been organized for the awareness raising in all sectors of the Portuguese society
- Training courses have been specifically organized for the technical staff of the public administrations through the Instituto Nacional de Administração (www.ina.pt)
- The Ministry of Education has created a specific initiative for students (www.crie.min-edu.pt)

Additional content can be obtained in the Web sites mentioned.

National government as user of information systems

Recent awareness programmes and initiatives

The initiatives of the government in this area have been rather limited.

However in May 2006 during the International Telecommunications Day, a decision was taken to dedicate the day to cybercrime. A special event had been organized including speakers from the Public Administration, the ENISA Portuguese representatives and the industry. The media have given significant coverage to the event.

Due to the success of the event, the organisation that operates the CERT – FCCN (www.fccn.pt) has recently signed a contract with a governmental funding agency to increase the number and scope of activities for the media.

Refer also to the *Gov. as Developer* section for more information on initiatives aimed at the public administration.

Local government as user of information systems

Recent awareness programmes and initiatives

Local governments, due to the nature of the political organisation of the country, have no activities in this area.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

Up to now there are no significant initiatives related to awareness raising promoted by the government.

Software vendors and resellers have some initiatives to raise awareness of information security issues but the government has not been directly involved.

Internet Service Providers (ISPs)

The cooperation between government and ISPs has not been directly organized by the government but through FCCN, the organisation running the Portuguese NREN.

In Portugal there are a number of ISPs and in recent years there has been a significant increase in the use of broadband technologies (cable and ADSL). Also there are an increasing number of hotspots where broadband access is available. Due to the nature of these technologies, ISPs have been active in distributing information to it's customers of the specific problems of these technologies due to the increasing potential of problems as a result of always-on networks and higher available bandwidth.

FCCN has organized, for around 2 years, periodic meetings with ISPs to discuss measures to be taken by this economic sector to control security problems. For ISPs the most relevant problem is SPAM and the problems related to malicious mail. A Forum has been created where ISPs share information about security problems and the techniques and solutions each of them is taking to solve these problems. Although they are competing in the market this is an area where cooperation is understood to be beneficial.

A project is just starting to develop a platform for information sharing concerning black lists of spammers to be interchanged among ISPs. FCCN will be the coordinator of this project. Together with this initiative each ISP is launching (addressed to its customer base), some initiatives dedicated to awareness raising in the security area, namely with details of good practices in the area.

Media

It should be noted that the examples listed below use media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

Initiatives for the media have not been organized in a structured way but several events have been organized that have been covered by the media, namely the press. Thus the strategy followed has been to launch projects (e.g., CERT.PT which is financed by the government), with the project initiatives covered by the press.

A significant problem that exists in this sector is that typically only the press (specialized and non-specialized) follow the events. Television, which could have a much broader outreach, has not covered any of the activities despite the efforts undertaken.

The creation of the Cybersecurity day, where specialists from the government and industry have been present, has been the most visible initiative since it has been chaired by the Minister responsible for this area. It is planned that more projects related to awareness raising will be continued in line with this initiative.

Also specialized magazines (for computer professionals) are dedicating some attention to this topic; specialists have been preparing articles related to network security issues.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Due to the high use of Microsoft platforms, the government has signed a cooperation agreement with Microsoft and FCCN for the exchange of security information about computer security. This agreement has recently been signed (July 2006) and it is expected to have a significant impact in the areas of awareness raising and education of users.

The reason for establishing this cooperation between the government, Microsoft and FCCN is related to the exploitation of the synergies among these entities.

The initial step will be the monthly publication of reports with security information related to attacks, threats and approaches to face them. The reports will be published in the Microsoft site and at the CERT.PT site (www.cert.pt). Press releases will be issued on a periodic basis to try to make this information available to a wider audience.

Future public-private partnerships

There are plans to launch similar initiatives with other players in the sector but no agreements have been finalized up to now and information can not be disclosed at this moment.

Government as partner with civil society

Recent awareness programmes and initiatives

There are no activities yet addressing the home public directly. This has been done indirectly with all the initiatives described in the previous sections.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

The only metrics in existence are those originating from the Portuguese CERT (www.cert.pt) with a classification of the security incidents that have been reported to the CERT.

Also there are metrics from the ISPs but they are reluctant in distributing this information to the general public.

Importance of Metrics/KPIs

It could be useful to create some common metrics but due to the dynamic nature of security problems, these metrics are constantly outdated.

24. Slovakia

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Slovakia have been detailed:

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as partner with civil society

Metrics and key performance indicators (KPIs)

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

There is no information available on awareness raising strategy conducted at a national level at this moment in time.

Legal, regulatory, and institutional arrangements to raise awareness

There are plans to create an informative CD or an online version covering subjects such as awareness raising in information security and technical dictionaries. As well as these, there are initiatives for educational projects aimed at targets such as government technicians and lawyers.

The Commission for Information Security was established at the end of 2005 as an advisory body for the Government Plenipotentiary for Information Society and includes relevant experts from the government, academia and the private sector.

National government as user of information systems

Recent awareness programmes and initiatives

To date there has not been any official programme with regards to raising awareness in users of the national government.

Local government as user of information systems

Recent awareness programmes and initiatives

To date there has not been any official programme with regards to raising awareness in users of the local government.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

Currently there are no ongoing initiatives with regards to raising awareness for the SME target group.

Internet Service Providers (ISPs)

Currently there are no ongoing initiatives with regards to raising awareness for the ISP target group.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

Currently there are no ongoing initiatives with regards to raising awareness for the Media target group.

There are plans to address the general public through media channels such as TV, newspaper and radio. These channels are considered most effective in being able to deliver messages to promote a culture of security.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Technical universities are utilised to educate young people in the field of security culture and are able to educate the general public through several training and education programs.

Possibilities also exist to make some education programs in cooperation with the private sector.

Future public-private partnerships

Partnerships are planned with the academic sector to work on educational projects in the field of information security.

Government as partner with civil society

Recent awareness programmes and initiatives

There are plans to create an informative CD or an online version covering subjects such as awareness raising in information security and technical dictionaries. The main target group will be the Home User and the main media channels used will be TV, newspaper and radio.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

Partnerships are planned with the academic sector to work on educational projects in the field of information security.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

As there are no official awareness raising initiatives in the country, there are no opportunities to use metrics or KPIs. In the future it is planned to use them to help gauge the success of the campaign.

25. Slovenia

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Slovenia have been detailed:

Current Situation

- Slovenia boasts a share of Internet users that is higher than in many EU member states. According to data provided by the *Statistical Office of the Republic of Slovenia*[16], in the first quarter of 2005 more than 840,000 people aged between the ages of 10 and 74 regularly (in the last 3 months) used the Internet. Of those, 440,000 were men and 400,000 women. In the first quarter of 2005, 87% of households had at least one mobile phone, 61% had a personal computer and 48% had access to the Internet. Of these, 40% had a broadband connection (e.g. ADSL, cable, UMTS). The percentage of the households with Internet access in Slovenia was equal to the EU-25 average. In the same period, 50% of the population aged between 10 and 74 regularly (in the last 3 months) used the Internet, while 12% of the population had already bought some goods over the Internet
- Slovenian children have a great deal of access to the Internet. Approximately 40% of the children/young people in the population between the ages of 10 and 15 use the Internet every day or almost every day. Approximately 33% of children/young people use the Internet at least once a week. Around 8% of children/young people use the Internet at least once a month and around 2% of children/young people use the Internet less than once a month[17]

The data is well accepted as it implies high development potential for Slovenia on one hand, but raises some concerns as well on the other, namely the issues regarding the safe use of the Internet and concerns about exposure of youth to harmful and illegal content. The Euro-barometer study 2004[18] provides a deeper insight into these issues:

- Around 53% of Slovenian parents report that they implement regulations for using the Internet (EU - 25 average: 45%). Rules can be divided in to five categories: privacy, restrict indecency, transferring files, time restraints and reporting if uncomfortable
- Almost 46% of Slovenian families say they do not feel the need to be more educated about harmful and illegal content on the Internet
- The results of the RIS survey, conducted in 2004[19], show that around 54% of Slovenian parents expressed concern about the safety of their children using the Internet. However, the public awareness of the problem of harmful and iilegal content produced by the Internet and new online technologies is still relatively poor. It is

[16] Statistical Office of the Republic of Slovenia: ICT use in households, 1st quarter 2005 in: http://www.stat.si/eng/novice_poglej.asp?ID=893

[17] RIS research: Survey on ICT usage in Households and by Individuals 2005 at: (http://www.ris.org); The results will be publicly accesible within few months.

[18] EuroBarometer (2004): Illegal and harmful content on the Internet in: http://europa.eu.int/information_society/activities/sip/docs/pdf/reports/eurobarometer_EU25_highlights.pdf

[19] RIS report: Web activities 2004 at: http://www.ris.org

interesting that 52% of Slovenian families believe that their children know what to do in a bad online situation (EU - 25 average: 60%)

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

There is no well defined programme that could be called a national strategy. However there have been some government supported activities aimed at enhancing public awareness on the increasing number of information security breaches and threads. The bottom up approach adopted to solve the problem has prevailed in the past. In the absence of a clear strategy it was believed that at least some synergic effects would be seen by supporting the different initiatives and activities by various parties. The government is aware of the problem and tries to be proactive, but its activity is somewhat proportional to the size of the problem. For example, phishing is not an issue in Slovenia yet so there is no need to launch a broad campaign that would solve a practically non existing problem.

Legal, regulatory, and institutional arrangements to raise awareness

From the legal perspective, Slovenia recognizes electronic communication and electronic forms. The legal and regulatory arrangements used stipulate and define the use of specific means for achieving appropriate security levels, with the focus on both the business and the government sector. The regulatory framework arranges security issues on different levels. Most commonly the security aspects are delivered through regulations on protection of consumer rights, electronic business regulation and on electronic communication acts. There is also government specific regulation in place addressing security issues e.g. ZUP.

No specific campaigns at the national level have been defined to date. Usually, promotion and best practices are delivered using various methods including targeted research and knowledge dissemination projects (CRP). Examples include Računalniška kriminaliteta, workshops such as the NATO Advanced Security Workshop and public-private publications such as the Varnostni forum. The most common security issues are addressed as vertical themes on a specific field e.g. electronic invoicing.

Another degree of security provision is performed through service providers on two levels: as an out-of-the-box solution combined with enabling services (e.g. Internet service provision with AV and FW protection) or as an integral part of services (e.g. personal AV and FE on network level).

Internationally supported initiatives are performed through dedicated development or through European wide research and development projects.

The Ministry of Higher Education, Science and Technology, Information Society Directorate is responsible for the security of e-business and prevention of Internet misuse.

Segments covered include creating conditions for safe and efficient electronic commerce and to develop strategy and measures to combat Internet abuse.

Ministry of Public Administration has its roots in the Government Centre for Informatics RS (GCI) which was established in January 1993 with adoption of the Government of the Republic of Slovenia Act (official Gazette of the Republic of Slovenia, No. 4/93).

In carrying out its tasks, the Ministry of Public Administration co-operates with state organisations, international, domestic and foreign governmental and non-governmental organisations and specialized institutions from the field of ICT.

The Security and Protection Service is in charge of setting up an adequate policy for the security and protection of data. The policy serves as a basis for practical implementation and integration of individual processes into a common system of security and protection of data. It combines previous experience and solutions of individual institutions with: modern technological trends; current standards; standards in development; EU standards. In addition to integrating the security policy at state organisation and public administration level, the task of the security and protection of data is to implement in systems and solutions. Tasks also include the coordination of other performers (such as individual organisations, services and institutions), the supervision of the implementation and, depending on the results of the implementation, the formation of further orientations/actions.

Public Activity (entitled "Action Plan eGovernment up to 2004") comprises of several IT security oriented activities. These include the information security policy and the Certificate policies of Government Certification authorities SIGEN-CA and SIGOV-CA. Education and training topics in IT security were planned for the "eGovernment Action Plan 2005 - 2008".

The effectiveness of the initiatives is monitored by the four stage framework 0–4, which is built upon the methodology “eGovernment indicators for benchmarking eEurope”. The level which is achieved at the moment is defined as current level “CLx” (where x stands for level 0-4) while the level to be achieved is defined as target level “TLx”.

Some parts of the “Action Plan eGovernment up to 2004” could be considered as good practice because they follow international standards. For example, the information security policy is compliant with ISO/IEC 17799. Furthermore, the Certificate policies of Certification authorities SIGOV-CA and SIGEN-CA are based on standards such as ETSI TS 101 456. A document has also been published entitled “Security requirement for applications using digital certificates”.

Police

As a constituent body of the Ministry of the Interior, the Police Force performs the tasks within organisational units set up at the national, regional and local levels. The General Police Directorate (GPD) which consists of ten internal organisational units is operating at the national level. There are 11 regional police directorates operating at the regional level, while 99 local police stations are operating at the local level.

A Computer Crime Division is a Police Force organisational unit to combat computer-based crime. Organisational units at regional levels are involved in investigations of serious and organized crime using IT such as hacking or defacing websites, making a web service unavailable or by being involved in computer virus outbreaks.

The Police also have some permanent activities that can be used to enhance public awareness about the information security issues. Usually, after the conclusion of an investigation of a more complex criminal case related to cybercrime, interviews are often given at press conferences by the official police representatives. Subject related press releases are often published to the press and on the net. Police experts have also given lectures at various conferences related to information security. A leaflet entitled "Ali se zavedate nevarnosti Interneta?" (Are you aware of the risks on the net?) is being currently being created.

Primary and secondary school

Teachers gather specific knowledge related to information security issues at various seminars which are primarily intended to foster the use of information and communication technologies in the classroom. There is a special group of teachers, so called "multiplikatorji" (i.e. multipliers), which are specifically educated and qualified by the National Education Institute of the Republic of Slovenia (http://www.zrss.si/) for education of other teachers. Among other topics related to ICT, this special group of teacher's knowledge transfer security related information. There are several other institutions in the school field in Slovenia that are active within the framework of European programmes such as Comenius, Leonardo da Vinci, Gruntvig and eLearning. Many of projects within the programmes include themes related to information security. Within Slovenia, the information security policy is almost exclusively prepared by ARNES (Slovenian NREN).

ARNES

Providing services of the SI-CERT, the body was identified by the former Slovenian Ministry of Information Society (MIS) as a centre of expertise in the fields of network and information security. As MIS recognised growing importance of network security, a project was drafted and assigned to ARNES. The project enabled the construction of a detailed knowledge base which is structured with different views on problems and solutions depending on the target audience (e.g. general public, technical personnel of ISPs and law-enforcement).

SI-CERT

The Slovenian Computer Emergency Response Team was established in 1995 within the Academic and Research Network of Slovenia (ARNES) with the goal of providing a central point for coordinating network security incident handling. Both the institutions as well as individuals are served by SI-CERT services.

On average, SI-CERT handles around 100 incidents each month. In order to provide its services, every CERT has to accumulate substantial knowledge related to various security issues. This knowledge is used while investigating incidents, in a direct advisory role, or to perform particular awareness raising activities for the community. Awareness raising activities include bulletins and advisories.

Bulletins and advisories are SI-CERT publications which relate directly to security problems directly observed in the community. Advisories are brief summaries of newly-discovered vulnerabilities, along with available workarounds and solutions. Advisories target both the general public, as well as system administrators.

Bulletins are more general articles, describing a particular type of a security problem, with more extensive background. Bulletins are geared more towards the general public, but provide references to technical details also. Examples of SI-CERT bulletins include articles on phishing and auto diallers. The aim of a bulletin is not so much to provide specific technical remedies for the problem, but more to raise awareness about a particular problem and suggest actions or behaviour that allows the user to avoid certain risks. This is often done through lectures or presentations.

Team members of SI-CERT use various opportunities to reach out to various segments of the community with the intent of presenting security issues and thus raise awareness on the subject. Lectures and presentations include local public events, as well as specialised courses for teachers in primary and secondary schools that disseminate information further to other teachers within a region.

University of Maribor, Faculty of Criminal Justice

The work of the Faculty of Criminal Justice is spread across six departments: social sciences; law; information science and methodology; criminal investigation, criminology and criminal law; security studies; and management and police administration. The departments are responsible for teaching work and, together with the Institute of Criminal Justice Research, make a significant contribution to research into security study issues in modern societies; members of the departments also offer consultancy and training services to various areas of the security system. The information science and methodology department covers information science, statistics and methodology. The main purpose of the department's work is to provide students with the basic knowledge they will need to approach scientific research work and analyse security phenomena. Another important function of the department is its work on databases and applications for research projects. The department also provides information support for the entire study and working process of the faculty, as well as study and education from various areas of information security. The faculty of Criminal Justice offers for the first time the possibility of the specialist study of information security. The study focuses on all aspects of information security threats and the tools for prevention of such threats.

The targeted groups are graduate students (of almost any area) who will use information systems as primary tools, and individuals who are already employed and work in the areas where such knowledge is mandatory.

National government as user of information systems

Recent awareness programmes and initiatives

There are no specific IT security awareness national-level programmes, as security issues are most commonly addressed through legislation or through specialized programmes performed by individuals or joint ventures between industry and the governmental sector. Security culture is also being developed through “themed” initiatives in different sectors such as trusted and secure electronic business.

An example of an individual security awareness initiative is the promotion of key governmental public infrastructure on its own and through different e-government or e-business services. Individual awareness programmes have been addressed as a result of targeted actions such as NATO Advanced Security in Networking Workshops for the region. Also, joint ventures between governmental and industrial sectors have been defined in the past, mostly as technical cooperation (e.g. e-Slog or moja.posta).

The security culture is being monitored through market and technology research by individuals and by governmentally funded programmes such as Raba Interneta v Sloveniji (RIS). Security issues are becoming an integral part of the information society infrastructure and should be promoted as such. Consideration of information security is thus a parallel or integrated thematic section in programmes such as e-health, e-government, e- business and e-learning.

Local government as user of information systems

Recent awareness programmes and initiatives

There are no specific programmes or initiatives aimed at raising awareness of users in local government.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

At least two cases exist on the technology level: Governmental CA being promoted as the most commonly used PKI enabling infrastructure for e-government and e-business services and the Slovenian Chamber of Commerce project, e-Slog, for a common business message standard through national support. As part of secure e-business initiatives, the security section was covered in terms of guidelines and technical recommendations for trusted business message exchange. The e-Slog initiative was a joint venture between industry and the governmental sector (DURS, CVI/MJU) for setting up information at a national level through a technical portal aimed at promoting trusted electronic business. The initiative is now overseen by GS1, a local EAN group.

E-government services are another example for industry and governmental cooperation in conducting B2G, e.g. tax declarations based on security services of national and commercial CSPs. E-government services are also promoted in C2G.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

There has been no specific nationwide media promotion by the government. There has been some targeted promotion by the Association for customer rights, certain public sectors (e.g. CVI/MJU) and by private organisations (e.g. IDC).

Government as partner with civil society

Recent awareness programmes and initiatives

SAFE-SI awareness Node (**http://www.safe.si**)

The Slovenian Government, especially the Directorate for Information Society within the Ministry of Higher Education Science and Technology, actively participates in the "Safer Internet Programme (http://ec.europa.eu/information_society/activities/sip/index_en.htm). As part of a coherent approach by the European Union, the initiative aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user. The Directorate for Information Society within the Ministry of Higher Education Science and Technology is a member of the SAFE-SI Advisory Board (http://www.safe.si). The *SAFE-SI* (Safer Internet Programme in Slovenia) is a *Slovenian national awareness node* that promotes and supports awareness aimed at the protection and education of children and teenagers using Internet and new online technologies. Partners in the consortium *are University of Ljubljana, the Faculty of Social Sciences and ARNES*. The project is co-financed by the Information Society and Media Directorate-General within European Commission.

The Programme started on 1st March 2005 and ends on 28th February 2006.

The Slovenian government will continue its participation in the Safer Internet Programme by co-financing the establishment of a hotline (STOPLINE.SI) for dealing with reports of illegal and harmful content on the Internet in Slovenia. The hotline is seen as an important and necessary step in Slovenia, taking into account that such a hotline in Slovenia does not exist. The main reason for the establishing Slovenian hotline is to combat child pornography, criminally racist content and hate speeches on the Internet as defined in the Slovenian legal regulations. The project will start in September 2006.

The Slovenian Awareness Node SAFE-SI (http://www.safe.si) targets the following audience:

- children aged 7 to 12 years old
- teenagers aged 13 to 17 years old
- parents
- teachers

With respect to Internet access and usage, children are often more advanced than their parents. However, while the Internet provides a new world of educational opportunities, entertainment and useful information, it also provides access to some hidden dangers, which are not made totally aware to children and teenagers. The goal is to provide parents with tools to control and verify the correct use of the Internet made by youngsters at home as well as at school and to give them some psychological/pedagogical advice on the best attitude towards the Internet related risks they face. Correct information and awareness should improve their confidence in the Internet as a positive opportunity for kids and should prevent unjust prohibition to surfing on the net. The project also aims at providing educators with basic knowledge on the Internet. Training seminars are also offered to stimulate the use of the Internet at schools in order to exploit its potential as a collective tool of communication and cultural growth.

The SAFE-SI project is about raising public awareness of ICTs among youngsters by targeting parents, children and the teachers. The aim is to help educate and empower Internet users to be able to communicate in a safe way, and to recognise and avoid Internet fraud, crime, privacy abuse and unwanted content.

The campaign has been implemented on the philosophy that awareness should be raised without raising a fear. Awareness raising should thus promote a positive image. The message is that the Internet, as a whole is not harmful, but there are certain aspects of the Internet that might be. This message has to be transmitted to both adults and children. The activities of the project are oriented towards developing websites, preparation and dissemination of promotional materials (such as brochures and posters), organisation of media presentations and raising concern in the overall media coverage. The most successful initiatives were the following activities:

- Design of a website
- Story-telling competition 2005
- Dissemination activities
- Safer Internet Day 2006

The Safer Internet Day 2006 was a high-profile event in Slovenia. The celebrations and events organized by the Node generated a lot of media interest. As a result, Safer Internet day activities had national coverage through most TV, radio and press channels.

The Node's priority is to strengthen the cooperation with relevant Slovenian media (digital and traditional) in order to ensure a broad media coverage. This is to be done by treating the media channels as the audience and to discuss the topics of safer Internet use with them and in relevant TV or radio shows.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

For information on the RIS project (the leading source on information society issues in Slovenia), refer to: http://www.ris.org/index.php?fl=0&p1=276&p2=285&p3=&id=334

26. Spain

No information was supplied

27. Sweden

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for Sweden have been detailed:

Current Situation

According to an annual survey conducted by the National Post and Telecom Agency (under the auspices of TEMO)[20]:

- Since 2003, the Swedes have become more careful about their own Internet security
- Swedish households have to a greater extent learned to use firewalls and updated antivirus programs when they surf. During 2003, 23% of Swedish households had a firewall. In 2004, this figure had increased to 47%. 53% used an updated antivirus program during 2002. This figure had increased to 78% during 2004
- A survey[21] based on a stratified random sample drawn from 2000 companies and organisations with 50 employees or more found that:
    - 28% of Swedish organisations have experienced one of the following four IT related incidents in the last 12 months: security incidents resulting in information or system components becoming available for an unauthorized person to read, copy, modify or erase; security incidents resulting in a serious reconnaissance of the system; security incident resulting in the system or parts of the system becoming unavailable (a so-called Denial of Service (DOS) attack); security incident resulting in a serious outbreak of malicious code with considerable consequences for the organisation
    - Of those that had experienced one of the four IT security issues, only 4% had reported the incident to the police; 37% thought that reporting the incident could result in negative publicity for the organisation

[20] Refer to 2005_33_sakerhetsinfo_iternetanv.pdf

[21] Refer to sweden_survey.pdf

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The national information security strategy is very high level at the moment; however there is recognition that awareness is an important issue. The strategy would be realised through the work of several agencies. Specific actions on awareness include the National Post and Telecom's websites on Internet security and the establishment of the CERT Swedish IT-incident centre (Sitic). For more information, refer to:

National Post and Telecom Agency (PTS)
http://www.pts.se/Default.asp?Sectionid=&Itemid=&Languageid=EN

Swedish IT-incident centre (Sitic)
http://www.sitic.se/eng/index.html

It is also worth noting that awareness raising is often a natural part of the work plan in an agency or a business and would come about with or without a national strategy. Examples are consumer protection agencies, sector agencies (electronic communication, finical services etc.) and law enforcement agencies.

The Swedish Consumer Agency for example provides information on safe e-commerce, provides a tool to protect IT users from modem hi-jacking (which for a period of time was a very large problem), and provides the ability to measure the actual bandwidth delivered by an ISP. For more information, refer to:

Swedish Consumer Agency
http://www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646 (English)
http://www.konsumentverket.se (Swedish)

Swedish Consumer Agency: Safe e-commerce
http://www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646

Swedish Consumer Agency: IT and Internet
http://www.konsumentverket.se/mallar/en/lista_artiklar.asp?lngCategoryId=922 (English)
http://www.internetit.konsumentverket.se (Swedish)

Legal, regulatory, and institutional arrangements to raise awareness

Sweden has handled the legal framework by assigning different tasks to government authorities such as the Swedish National Post and Telecom Agency, the Swedish Data Inspection Board and the Swedish Consumer Agency. These authorities use legislation such as the Electronic Communications Act and the Personal Data Act.

Other agencies, such as SEMA (below) also have responsibilities.

Data protection Board (DIB)

The Personal Data Act has section 31-32 security for privacy protection. The Data Inspection Board has issued security guide lines and gives advice and seminars for the controllers of data and the public. To raise awareness the controller can use the guide lines as a general description of the measures that have been taken to ensure security.

In the Personal Data Act (PDA) there is a definition of what constitutes a personal data representative (PDR): "A natural person, appointed by the controller of personal data, who shall independently assure that the personal data is processed in a correct and lawful manner. The idea is that the PDR shall be an asset, a resource, for the controller in terms of privacy protection when processing personal data".

The DIB assists the PDRs with advice and seminars including security. By 28th April 2006, the controllers had notified and appointed 3467 PDRs and 80% of the local municipal administrations in Sweden have notified PDRs to the DIB. The PDRs are regarded as an “extended arm” of the Data Inspection Board.

National government as user of information systems

Recent awareness programmes and initiatives

There is little information about the effectiveness of the various agency or government initiatives; the below information should not be treated as an exhaustive listing of all the most effective measures. The main responsibility for the secure use of information technology lies with each agency.

Swedish Administrative Development Agency

Swedish Administrative Development Agency (Verva) is an expert in the field of public administration development. The agency promotes and supports public administration development and enhances coordination in the government administration including the procurement and use of IT. For more information, refer to: http://www.verva.se/web/t/Page____492.aspx

National Post and Telecom Agency

The information efforts by the National Post and Telecom Agency and by the Sitic agency have been referred to in the previous text.

Swedish Emergency Management Agency (SEMA)

The Swedish Emergency Management Agency (SEMA) arranges seminars, twice a year, together with other agencies in order to strengthen the society's information security and to raise awareness at management level at Swedish agencies. It also publishes a monthly newsletter. It has produced a DVD film with key public and private management figures to raise awareness at the higher levels within an organisation. SEMA is developing an interactive e-learning product to increase the knowledge within the information security area. SEMA also arranges courses within the area.

SEMA is also producing recommendations for a baseline security level. The defined level establishes a minimum security level for IT-systems necessary for essential societal services. The recommendations can be applied to public and private authorities. For more information, refer to:

http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/KBMs%20publikationsserier/Rekommenderar/bits_eng_recomm_2003-2.pdf

In order to implement the baseline security, SEMA has produced an IT security guide as an instrument for analysis of the security in IT systems. SEMA is also producing a yearly national risk assessment. For more information, refer to:

http://www.krisberedskapsmyndigheten.se/6193.epibrw

Local government as user of information systems

Recent awareness programmes and initiatives

It has not been possible to explore individual local governments which number around 290. Some details captured are as below.

The Swedish Association of Local Authorities and Regions

The Swedish Association of Local Authorities and the Federation of Swedish County Councils represent the governmental, professional and employer related interests of Sweden's 290 local authorities, 18 county councils and two regions. For more information, refer to http://kikaren.skl.se/artikel.asp?C=756&A=180

The association and the federation strive to promote and strengthen local self-government and to create the best possible conditions for the work of their members. Membership fees largely finance the activities.

The association has published information on information security policy adapted to local and regional authorities. Security issues are discussed at conferences and best practice from a local authority could be highlighted. Information such as advice on new and relevant legislation is published on the website.

City of Stockholm film initiative

Citizens must be confident about how their personal information is handled and how services are offered. They rely on the fact that the City of Stockholm employees are well trained and aware of the importance of security when delivering the services.

The City of Stockholm has made a film based on the new policy and guidelines for Information Security (decided during autumn 2005). It is an attempt to make the end users aware of what information security is about from their own perspective. The film contains a number of interviews with employees and some partners to the City of Stockholm; every interview is based on a chapter from the new policy and guidelines.

The chapters of the guidelines and as illustrated in the film cover areas such as administration, responsibility and methods as well as more technical subject areas.

One topic covered includes the social welfare system which is one of the most important systems for the City of Stockholm. Some employees describe their role specific responsibilities. These include amongst others a System Owner, a System Administrator and a local Handling Officer.

Physical security or perimeter security is another issue described in the film; aspects of mobility such as working with hand-held computers and the risk of using wireless connections are covered

A Risk Analysis exercise from a local borough in the city is also presented. The chapter emphasises the importance of eSecurity and the necessity of having top management supporting the work.

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

National Post and Telecom Agency

The National Post and Telecom Agency hosts websites with information on Internet security. The websites are typically aimed at households and the public/private sector (especially smaller companies or agencies that have limited resources for information security at their disposal). The content also includes interactive testers for a specified computer (conducted on-line) as well as interactive education programs on passwords.

The Swedish IT Incident Centre (Sitic) in 2005 conducted the survey “Underreporting of IT Security Incidents – Hidden statistics on IT Security incidents in Sweden”. The purpose of the study was to collect up-to-date information on the extent to which typical IT security incidents are experienced by Swedish organisations, to what extent such incidents are internally reported to the organisation’s security departments, to what extent IT security incidents are externally reported to the police and to Sitic, and the reasons behind the willingness to report such incidents to the police and to Sitic.

The hypothesis of the study is that underreporting can be traced within four areas: routines for outsourcing, routines for internal reporting, routines for external reporting, and actual reporting.

The study is a co-operation between Sitic and the National Criminal Investigation Department. Temo, a market research company, has conducted the fieldwork. The survey is based on a stratified random sample drawn from companies and organisations with 50 employees or more. For more information refer to http://www.pts.se/Nyheter/pressmeddelande.asp?ItemId=4718

Refer to the *Gov. as Partner (Society)* section for more information on the National Post and Telecom Agency initiatives.

Internet Service Providers (ISPs)

No information is available in a suitable format at this time. Many operators provide security information on their websites.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

It's likely that media would be part of many strategies in this area, however not necessarily as an end in itself. Media has in recent years reported on information security problems such as computer viruses, phising and so on. With a high number of computers in households, Swedish media probably has an interest in reporting certain issues by asking agencies and private sector experts for information.

Refer to the *Gov. as Partner (Society)* section for more information on the National Post and Telecom Agency initiatives.

Public-private partnership

ISO/IEC 17799:2005

The Swedish Standards Institute had published the ISO/IEC 17799:2005 in October 2005. Subjects covered include: Information technology, security techniques and code of practice for information security management.

The Data Inspection Board encourages public authorities, the health care sector, industry and standardisation organisations to develop and apply privacy controls and provide necessary confidentiality and security.

ISO/IEC 17799:2005 Section 15 Compliance with legal requirements has raised awareness in 15.1.4 Data protection and privacy of personal information. This standard has also been used as a model for auditing government agencies' internal work on information security.

Carelink – National cooperation to develop the use of IT in Swedish healthcare

Carelink works with supportive services such as SJUNET (a national broadband communication network), directory services and information security. Other important tasks include information and diffusion of best practices and good examples. Carelink is a co-ordinating partner in national projects and networks, covering most of the perspectives that concern the development of IT in health care. For more information, refer to:

http://www.carelink.se/pages/newsbill.asp?VersionID=1&Pages=1,124

Government as partner with civil society

Recent awareness programmes and initiatives

National Post and Telecom Agency

According to the National Post and Telecom Agency's annual national survey ("Individundersökningen"), 78% of Swedish households have access to the Internet at home. The latest survey was carried out in September and October 2005, by a postal questionnaire to 4000 randomly selected Swedes in the age range 16–75 years. The survey was implemented 2002.

During the period December 2002 to August 2005, the National Post and Telecom Agency was assigned by the government to compile information about Internet security, and make this available to Internet users.

The strategy was to supply the target groups with easily accessible, target group adapted information in one main channel. The ambition was also to offer information via one complement channel and to spread information via selected organisations for greater range and cost efficiency.

In a later stage of the assignment, resources were also devoted to market the information in banner campaigns for maximum range.

The target groups were:

- Home User
- SME
- Small and medium sized government authorities

The overall objective has been to enhance the awareness and knowledge of the target groups regarding security on the Internet so that they will use the Internet in a more secure way and not expose themselves or others to unnecessary risks.

In November 2003, the National Post and Telecom Agency launched an Internet security website, (www.pts.se/internetsakerhet), and an interactive course together with printed material. The printed material consisted of information cards (with stands), brochures with good tips and special feature issues of the agency's magazine. A new version of the website including an interactive web assistant and a new web service for consumers to test security of personal computers was launched in mid-April 2005. The National Post and Telecom Agency also conducted a web campaign to market the website and service.

The printed material was distributed to local consumer advisors, libraries, schools and universities, different trade organisations, ISPs, banks and municipalities. Media was also supplied with information about Internet security via press releases and direct contacts with journalists.

The topics on the website targeted to two categories of users: Home User (För hemmet) and for the workplace (För arbetsplatsen).

The Home Users can find information on the following topics: About the Internet, Connection, Surfing, E-mail, Download, Sharing files, Chat, Network games, Do bank errands, E-shopping, Fifteen good tips, Learn interactively, Common questions, Common terms and other Links.

The following information is provided to the workplace: Prepare policy, Rules for infrastructure, Connect to the Internet, Configure systems, Create safety copies, Connect at distance, Connect to business partners, Protecting against harmful codes, Managing IT incidents, E-identification and transactions, Buy security services, Good tips for the workplace and other Links.

The result of the service and activities were (a final report describing the entire project is available in Swedish with a summary in English):

- Over 180,000 tests were conducted through the web-based service computer security check. Refer to www.testadatorn.se and http://www.pts.se/Nyheter/pressmeddelande.asp?Itemid=5201
- There were over 250,000 visits to the website
- There were 30,000 visits to the interactive course on the website
- In June 2005 the website was awarded “Website of the month” by Sweden’s largest home computer magazine, PC för alla
- Over 25,000 questions have been dealt with by the virtual web assistants
- There have been over 150 press clippings
- 100,000 information cards with table stands have been distributed
- 60,000 brochures “Surf Securely” have been distributed
- 10,000 magazines “Get Connected” have been distributed
- The Swedish Consumer Agency and the National Post and Telecom Agency have, together with several operators, implemented a joint information initiative regarding modem hijacking
- The National Post and Telecom Agency has in 2005 together with 14 other organisations, participated in SurfaLugnt – a national campaign about Internet security

The National Post and Telecom Agency has decided to incorporate the awareness campaign in the authority's everyday work after the ending of the government project. Many of the strategies, target groups and messages are similar and so can be reused.

In November 2005, the National Post and Telecom Agency launched a password tester (www.testalosenord.se). The test teaches how passwords should be constructed to become strong and difficult to crack. The expectation is that the target groups will use this knowledge when they create passwords at home or at work. On the website, the message is that the test should not be used to test passwords already in use or to create new ones. It should only be used to test different sign combinations to see if they would be strong or weak if used as passwords.

The National Post and Telecom Agency also conducted a banner campaign to market the web services that are available on the Internet security website – computer security check and password tester. The campaign period was six weeks in October and November 2005. Click-thru-rate was 0.15%, which according to the media advisors is a very good percentage. Campaign related visitors were at 84,000.

Both tests have been successful. At the beginning of April 2006, over 250,000 password tests have been conducted. The computer security check has performed over 410,000 tests. The Internet security site has had over 600,000 visitors.

In addition to the awareness program described above, the National Post and Telecom Agency has also produced two reports covering the subjects of security threats to mobile telephony and spyware:

Report: Security threats to mobile telephony (PTS-ER-2006:18)

This report describes security threats to mobile telephony from a user perspective and contains an assessment of the situation in the winter of 2005/2006. This report is based on interviews with operators, mobile telephone manufacturers, security companies and other experts within the field together with a workshop where the above-mentioned advisers gathered to jointly evaluate various possible security threats to users of mobile telephony. The report focused on the GSM and UMTS technologies.

The risk of security threats to mobile telephony is currently considered to be small. According to the mobile operators, only a few cases of mobile telephones that have been infected by harmful codes have been found. However, a number of general trends can be discerned, which in the future may lead to increasing security risks for mobile telephones and mobile telephone users. The mobile telephones of the future will increasingly resemble PCs. They will contain valuable information, their performance will increase; a mobile telephone will have an interface in relation to several different kinds of communications networks and be continuously connected to a data network. In addition, more telephones will offer an open development interface that independent developers can use to develop new applications for mobile telephones. These trends result in the mobile telephones of the future becoming, to an increasing extent, more vulnerable. Harmful codes will especially become a major threat to security when smart telephones, which use open operative systems, become more common. Critical factors for this development are that:

- smart telephones achieve increased penetration (estimated to be 10% in 2007)
- transmission rates between mobile telephones and data networks increase
- more mobile telephones become continuously connected to data services (GPRS, UMTS, WLAN, etc.)
- increasing numbers of communications services have fixed charges

PTS expects that the stakeholders in the market will cooperate to minimise security risks for mobile telephony and make use of the experience and knowledge regarding security problems on the Internet to, as far as possible, avoid the same problems adversely affecting mobile telephony. Besides the above, the main measure that can minimise the risk for future security threats to mobile telephony is to increase the awareness of users about security risks and how they can protect themselves against them.

Report: Spyware and closely related phenomena (PTS-ER-2005:15)

In pace with society continuing to develop into an information society, where large sections of both business and government are to varying degrees dependent upon computers and communications networks, an increasing dependence arises on these computers and networks operating and being secure. For many years viruses and other harmful codes have constituted a much-noted threat to such functions. However, there are also programs and technical systems that in ways other than by pure destruction may constitute a threat to both the functionality of the communications networks and the trust and confidence which users have in their use. This report is aimed at a group of such programs that in various ways may constitute a threat in the form of functions that violate privacy; everything from more harmless storage of menu choices in cookie files to the actual kidnapping of entire networks of computers. The programs and their functions can in individual cases entail serious violations of privacy for the individual user but may also in a broader perspective constitute a threat to public confidence and preparedness to utilise electronic communications services. A further problem is also that some of these programs facilitate malicious parties, via remotely controlled computers, creating platforms for further attacks of which the user is entirely unaware.

The section regarding spyware is generally addressed to everyone who has an interest in knowing about these phenomena and who, on a less technically-orientated level, wishes to obtain an overall awareness of their occurrence, potential threats and the possibilities of protecting oneself. The section regarding legal issues is mainly directed at lawyers or others who are interested in the legal issues that, primarily on the basis of the Electronic Communications Act (EkomL), arise in conjunction with the occurrence of spyware.

Public-private partnership

The SurfaLugnt national campaign for a safer Internet is one of the most successful partnerships between the IT industry and relevant authorities. For more information, refer to http://www.surfalugnt.se

The partnership leveraged respective expertise and access to channels and was formed as an alliance is viewed as being more credible and has more opportunity of gaining attention among the target groups and the media. In 2006, the campaign will change from “why to how” and focus more on the Young.

A project plan for April 2005 to December 2005 was agreed with the stakeholders, and a Code of Conduct was created as part of the project contract. A design guide was also presented.

The initial plan was for the campaign to reach 100 towns – a year later the number was 200. Also, the original 1500 activities planned turned out to be 2000. The some 2000 contact people are double the original expected amount. The website has had 300,000 visitors with a target population of 1.5 million.

The partners involved in the initiative are:

National Post and Telecom Agency, Swedish Emergency Management Agency, 24/7 Agency Delegation, Swedish Bankers’ Association, Swedish Confederation of Enterprises, Foundation for Internet Infrastructure, Swedish IT & Telecom Industry Association, F-Secure, Microsoft, TeliaSonera and Symantec. The Data Inspection Board and IBM participated as minor financial partners.

For more information, refer to ppp_for_a_safer_internet.pdf.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

National Post and Telecom Agency

The National Post and Telecom Agency has used the agency's annual national survey ("Individundersökningen") to follow up on different campaigns. The survey has not been designed specifically to evaluate awareness projects, none-the-less, it has been useful in this matter. The latest survey was carried out in September and October 2005, by a postal questionnaire to 4 000 randomly selected Swedes in the age range 16–75 years. The survey was implemented 2002.

Among many other things, the survey measures the usage of firewalls and antivirus software (with an update function) in Swedish households with Internet connections. The National Post and Telecom Agency launched the Internet security website in November 2003. One of the messages on the website has been that Internet users should use both firewall and antivirus software, and to keep them updated.

In December 2003, the survey showed that 34% used a firewall; the figure had increased to 47% in 2004 and 64% in 2005. The corresponding figures for antivirus software with an update function are 66, 78 and 80% respectively.

The Awareness Campaign Surfa Lugnt

SurfaLugnt has measured knowledge status and attitude of the SME and Home User target groups. Quantitative targets have included the number of activities undertaken, the number of places that were visited and number of people involved.

From a government perspective, the primary interest of metrics would be to have a way of measuring the effects of different awareness raising initiatives. This would then be used to assess the value of the initiatives and the resources put to them, as well as making them more successful.

Lessons Learnt

ENISA has facilitated lessons learnt sessions with delegates of PTS and the Swedish IT & Telecom Industry Association.

Website by the National Post and Telecom Agency

Challenges of the project

- Wide scope of the project (i.e. number of target groups)
- Use of different languages for different target groups

What worked well

- Collaboration with SITIC (CERT community) to develop technical material
- SITIC knowledge at disposal
- Experts signing-off content before lunching the website
- Different points of entrance for the website
- A lot of content available
- Use of the web as a channel
- Starting activities a while before the lunching date of the website
- Project team (5/10 people)
- Analysis of target group prior to the campaign - this has been done through interviews and not through a survey. People have been interviewed to gather information about their needs/ knowledge. An external company has been involved in this activity (marketing approach)
- Involvement of media - in the first phase of the project press releases and banners were used. Banners were primarily for smaller companies and consumers to use on their websites - media was note used
- In the second phase, due to an increase in the budget, a web campaign has been put in place allowing for paid advertisements etc
- Measurement of the click rate and navigation by surfer of the website
- Distribution of printed material (i e brochures) to schools, libraries etc.

What didn't work well

- Team not fully dedicated (regarding time) to the project
- Lack of expertise – difficult for information officers to understand/update information related to SMEs. Updating content for Home Users was easier
- SITIC not always available to work on the project

- Assess level of awareness before launching the campaign. This had not been done due to a lack of funds and because it was believed that the initial analysis was enough to picture the situation
- Lack of identification of categories within the target groups (e.g. Young)
- Reaching the Young - they use a different language, they have different needs
- Maintenance of tools developed by different sources: “Security check” (firewall) is based on an open source software call Nessus; “Password tester” is partially based on an open source software call CrackLib
- Advanced tools unavailable to the users

Notes for future campaigns

- Need to clearly identify number of resources involved/dedicated to the project
- Assess level of awareness before launching the campaign
- Limit the scope and number of target groups
- Focus on consumers and bigger threads
- Target the Young
- Buy media - require more media involvement
- Develop a tool to be used by the users or offer something to the user (e.g. a tool to test your laptop). Ideally downloadable software should not be used as requires more maintenance
- Have a dynamic website
- Further detail the target groups – channels used for Silver Surfers are typically different
- Involve the ISPs
- Resources should be available to keep material up to date
- Having a plan after the launch of the campaign. Define roles and responsibilities for the following managing the campaign and adjusting it if required

SurfaLugnt (2005 and beginning of 2006)

What worked well

- Having a project manager (PM) - a PM generates ideas, is operational and tackles many of the problems that arise. A PM drives the campaign much more effectively
- The steering board worked well despite the number and the different partners involved
- Expertise of people involved: 12/15 partners were involved. Each organisation had its own expertise to contribute with
- Synergies with what exists already - there are often good advice, tests and other practical information around which can and should be incorporated

- Local/regional dissemination - if you really want to change behavior of users with the help of a limited number of resources it is key to find local partners (also opinion makers/ambassadors) and to involve local networks for the target groups
- Website organised by local/regional areas - the website is a very important tool to communicate ideas, facts, information tools etc. If the user can recognize what is happening in his or her area, it may be easier for them to decide to join any activity/event/discussion which is advertised
- Too much content was not developed
- Practical advice given to the users - provide clear messages. Target groups appreciated comprehensive information
- Build a website first and then had developed a public-private partnership
- Define roles and responsibilities
- Website as a channel – cost effective tool for working on a national level campaign with limited resources and very large target groups

What didn't work well

- No full time PM
- Media attention was insufficient – it's very important for the campaign stakeholders
- Number of ISPs involved in the project was not as expected
- Insufficient partners and associated expertise - for example, there were a lot of questions related to payments over the Internet but the project was not able to handle them as the group was lacking banking expertise
- Lacked understanding of target groups – time pressure did not allow addressing target groups in an appropriate way. The communication used was not always appropriate (e.g. for SMEs)
- Quality of material produced
- The contract was limited to a one year operation. In order to continue the activity in 2006, it has been necessary to have a new contract in place

Lessons Learnt for current campaign

- Understand the target groups to have a better impact
- Change activities from the previous year – from "why" to "how to handle"
- Develop better material - this year a movie for schools and presentations has been developed. Schools are used as multipliers, often involving parents
- Improve media visibility - media package developed to all Swedish papers this year
- Get professional support to develop media attention
- More flexible contract - the new contract signed by companies can be prolonged without new assignments (the annual plan is accepted by the payment). If only a few companies will be involved in the future, it is possible the project will close down. Long collaboration is foreseen

- Develop relationships with different multipliers (e.g. sports associations, senior silver associations, etc)
- Creation of working groups (WGs) which are helping the PM to develop ideas. This approach needs to be improved following a first assessment on the performance of the WGs

Notes for future campaigns

- Resources need to be available to keep material up to date
- Need to have a plan for after the launch of the campaign. It should define roles and responsibilities for the process, how to manage the campaign and how to adjust it if required

Campaign Initiatives

e-Security – City of Stockholm

As the public administration increase their service and contact with their citizens there is an increased demand for eSecurity. Citizens using the new services expect the same security, confidentiality and reliability as when they get the service over-the-counter. For citizens to accept and start using the new services they must have confidence in them and therefore eSecurity is a very important issue for all governments and local-governments.

The nature of today's global infrastructure also means that all cities are part of the new digital service-economy. Cities should understand the importance of eSecurity and to understand that they need to become more and more dependent on each other to be able to provide sufficient eSecurity.

There are a number of eSecurity initiatives but most within awareness raising programs towards citizens and businesses. With the increased pressure towards cities to provide a secure and confidential service, there is a strong need for cities to work together in establishing standards and sharing best practices within eSecurity.

SaferInternet - Youth panels a success story! (article)[22]

Summary

In order to disseminate knowledge of safer Internet use, the Swedish node has chosen to carry out a number of regional seminars: these are mainly targeted at teachers but also include other professionals working with children and youth.

One of the most successful and appreciated elements of the seminars is a youth panel showing how young people use and perceive new media.

Details

Despite the fact that children and teachers meet almost daily, teachers are most of the time completely unaware of how their pupils use new media such as the Internet and mobile phones in their social lives. For teachers the Internet is more a tool for information gathering than of communication. For youngsters, it is quite the opposite.

[22] http://www.saferInternet.org/ww/en/pub/insafe/news/articles/0706/sv1.htm, 31st July 2006.

At every regional seminar the Swedish node makes sure that the local partner has recruited a youth panel from schools in the region. They usually consist of six to eight girls and boys, aged 13-18. Their knowledge and experiences are shared with the audience with the help of a professional moderator.

Youths are asked to describe their everyday life on the Internet: chatting, visiting communities, doing homework and playing online games. They are also asked about problems like bullying, grooming etc. that they or their friends encounter and how they handle these issues. Topics like ICT education in school and the engagement of parents are also brought up.

As a rule, all teenagers in these panels are very eager to talk and proud to be the experts of the day. Being taken seriously and heard by adults is highly appreciated. The seminar item that usually gets the highest score in the evaluation is namely the youth panel. This proves that adults also find these testimonials truly valuable and that they are very interested in bridging the knowledge gap between generations.

SaferInternet - Swedish pupils and mobile phones (article)[23]

Summary

A Swedish survey gives insight on mobile phone use by children and young people.

Details

In the beginning of the spring term 2006 a number of school classes were asked to answer a web based questionnaire about mobile phone use. The classes contacted were the contacts in the project “the young Internet” which investigates the safer use of the Internet and new technologies. The questionnaire was answered by 130 pupils aged 10 to 18.

It was found that 97% of the pupils have their own phone and 80% of them use it daily. As expected, the most common usage is calling (90%) and sending/receiving SMS (78%). Other functions used were games (27%), photos (44%), MMS (21%) and email (4%). One out of four pupils had received SMS or photos that had made them upset, sad or scared. However, only 3% of them had told a grown up about it.

Another part of the questionnaire was about rules regarding the use of mobile phones in schools. One out of three pupils didn’t know if the school had any such rules.

[23] http://www.saferInternet.org/ww/en/pub/insafe/news/articles/0706/sv2.htm, 31st July 2006.

Even though mobile phones have become very common, more than one out of four of the phones do not have a camera and very few of the pupils have got phones with the latest features such as 3G.

28. United Kingdom

Based upon the responses to the questionnaire and on the supplemented information from interviews, research and additional material, the following sections for United Kingdom have been detailed:

Current Situation

- "Two thirds of British firms suffered a malicious incident through electronic means during 2004 - by June 2005 over 5.7 million bogus emails a day were being sent worldwide, seeking financial information to commit fraud"[24]
- The Information Security Breaches Survey 2006[25] commissioned by the United Kingdom's Department of Trade and Industry (DTI), states that:
    - Two-thirds of UK businesses had a security incident in the last year. More than half of UK businesses suffered a malicious incident
    - A third fewer companies had viruses than in 2004. However, the number of infections each has suffered has gone up and viruses still account for 50% of the worst security incidents (the single largest cause)
    - Despite greater increases in acceptable usage policies and restriction of Internet access misuse incidents remain at 2004 levels. Staff misuse impacts small businesses most – half affected cited it as the source of their worst incident
    - Despite the high priority attached to security and the growth in security and acceptable usage policies, many firms do not have a culture of security awareness

[24] Symantec Research, Management Today publication November 2005.

[25] dti_info_security_2006.pdf

Government as developer of legal, regulatory and institutional arrangements to raise awareness

National awareness raising strategy

The UK Government Strategy for Information Assurance was ratified in June 2003. It was produced by the Central Sponsor for Information Assurance within the Cabinet Office. The strategy deals with awareness raising in terms of partnerships between government, the wider public sector, businesses and the citizen to protect the social and economic well being of the nation. There are some 70 key action points in the strategy including outreach to the general public and advice to small businesses.

The strategy targets key areas such as central government, local government, industry and the citizen. To date the impact of the strategy has been significant with programmes such as the CSIA Claims Tested Mark (www.cctmark.gov.uk), Senior Information Risk Owner Programme (SIRO), Information Assurance Governance Framework, alerting schemes such as ITsafe (www.itsafe.gov.uk) and the awareness raising Get Safe Online campaign (www.getsafeonline.org)

Legal, regulatory, and institutional arrangements to raise awareness

Within the UK government, awareness raising of information security issues is becoming increasingly important. The Central sponsor for Information assurance (CSIA) works with partners across government including the Department of Trade and Industry (DTI), National Infrastructure Security Co-ordination Centre (NISCC), Home Office and Serious Organised Crime Agency (SOCA).

Through committees such as the Outreach Committee which reports to the Cabinet Office Committee on Security, awareness campaigns and forums are developed and shared to ensure a cross governmental approach to raising awareness of information security issues.

In its work to promote good information security management, DTI advocates the use of the international security standards ISO 17799 and ISO 27001 (which equate to the former British Standards BS 7799 Parts 1 and 2). These are risk-based standards, intended as management-based solutions. DTI views these standards as business enablers. Standards development continues: BS 7799 Part 3 on Risk Management was launched earlier in 2006. Further work is ongoing within ISO and in time it is hoped that within the international standards arena, there will be a “family” of information security related standards in the ISO 27000 series. DTI is closely involved at an international level in terms of security standards.

DTI's remit is with business. The Cabinet Office leads in terms of the implementation of standards within national and local government.

Standards background: In 1993, responding to demands from industry, the DTI set up an industry working group, made up of experienced information security managers. A Code of Practice for Information Security Management was produced later that year and this formed the basis of the British Standard BS 7799 Part 1, first published in 1995 and revised in 1999.

Industry also wanted a mechanism to allow for certification against BS 7799 that would provide an independent and credible means to demonstrate compliance. Accordingly, the DTI asked BSI (British Standards) to prepare BS 7799 Part 2, the specification against which a business is assessed to determine compliance with BS 7799 Part 1. BS 7799 Part 2 was also produced in consultation with UK business. It was first published in 1998 and was revised in 1999 and again in 2002.

In December 2000 BS 7799 Part 1 achieved the status of an international standard, becoming ISO/IEC 17799. This standard was revised in 2005 in line with normal ISO procedures. From April 2007 it will be renumbered as ISO/IEC 27002.

In 2005 BS 7799 Part 2 also became an international standard and is now ISO/IEC 27001. Many businesses may wish to obtain independent certification against ISO/IEC 27001 using third-party organisations such as certification bodies. Others may decide to use ISO/IEC 17799 as guidance to implement their own information security management system, without necessarily seeking certification.

The DTI's own influential 2006 Information Security Breaches Survey conducted by PricewaterhouseCoopers (see later) found that effectiveness and efficiency were driving the adoption of information security standards with companies and suppliers (rather than any desire for a “kite mark”). Of those companies using the standard 87% considered it had improved business continuity and 85% believed it had minimised damage to their company from security incidents. This is not now simply a UK phenomenon. The uptake of the standard since late 2005 when BS 7799 Part 2 became an international standard has shown a significant increase, especially in markets such as Japan.

National government as user of information systems

Recent awareness programmes and initiatives

National cross-Government awareness is being developed through the CSIA via key development programmes.

The document; 'Protecting Our Information Systems, Working in partnership for a secure and resilient UL information infrastructure,' was written and published in 2003. It identifies why information systems need to be protected, the risks facing information systems and why government is concerned with protecting all information systems. The document is available to download at: http://www.cabinetoffice.gov.uk/csia/documents/pdf/CSIA_booklet.pdf

The programmes developed also include the Senior Information Risk Owner network - an initiative to establish senior departmental figures as owners of information risk. The programme works to educate the senior information risk owners to be increasingly aware of the importance of the key information assurance principles of confidentiality, integrity and availability and how they are applied correctly.

Another measure developed and implemented across national government is the Information Assurance Governance Framework. This document was published on the web on 22nd November 2005, it explains the process of IA governance and provides guidance on implementation and best practice for organisations across the public sector.

The document is available to download at:
www.cabinetoffice.gov.uk/csia/ia_governance/content.asp

A review of Information assurance initiatives was produced by an independent reviewer for the CSIA in November 2004. The report titled, 'Information Assurance: A review of UK Government and Industry Initiatives' provides an insight into the initiatives, strategies and policies that support the protection of information systems, identifying the work being done by organisations in both the public and private sectors.

A further measure in the awareness raising strategy is the Information Assurance Technical Programme (IATP). This programme is a cross-governmental initiative to investigate the information assurance requirements of departments, for departments to ensure information assurance is embedded into future product and service developments in information technologies.

The DTI's Information Security Breaches Survey, whilst aimed at business, is widely read across national and local government and informs much of the DTI's work with business. In 2006 efforts have been made to promote the Survey's findings at a more local level eg to Regional Development Authorities.

Local government as user of information systems

Recent awareness programmes and initiatives

Local governments have benefited from working with central government to adapt the Information Assurance framework, (www.cabinetoffice.gov.uk/csia/ia_governance/content.asp) in order to tackle the key issues appropriate to local government information assurance.

The CSIA Claims Tested mark (www.cctmark.gov.uk) is a quality mark for IT security and provides local governments with a confidence that the information assurance products and services that they use will perform exactly how they expect them to.

The CSIA Information Assurance roadshows took place across the UK in 2005 and 2006 and were extremely successful in delivering key information assurance messages across local government and the wider public sector network. These sessions allowed debate on the issues of Information Governance, information security standards, the CSIA Claims Tested Mark and the Institute for Information Security Professionals.

The Warning Advice and Reporting Points (WARPs) initiative, supported by CSIA and implemented through NISCC, includes the development of a local government WARP. The WARP initiatives create information sharing portals that can only be accessed by trusted members of that particular WARP. Further information (http://www.niscc.gov.uk/niscc/warpInfo-en.html) WARPs are part of the National Infrastructure Security Co-ordination Centre's information sharing strategy to help combat the increasing risk of electronic attack on the information systems.

DTI's ISO 17799 UK Users' Group has over 600 members, mainly from business but with quite a substantial number from the public sector. This group is run by an industry steering committee (DTI provides the secretariat) and regular workshops are held on various aspects of security with a major focus on the ISO 17799/27000 series of standards. The most recent regional workshop (May 2006) was hosted by a public sector member (Leeds City Council). A guide to the Users' Group is available from the Downloads section of the DTI website at www.dti.gov.uk/sectors/infosec

DTI is supporting the November 2006 Conference "Information Security and Business Continuity in the Public Sector ", the 5th event of its kind. See www.kable.co.uk

Government as partner with business and industry

Small and medium-sized enterprises (SMEs)

CSIA – British Chambers of Commerce roadshows are running from April 2006 until November 2006. The roadshows highlight internet security issues and promote initiatives such as CCT Mark, Get Safe Online, ITSafe, NISCC WARPs, IA governance and SIRO programmes to small and medium sized businesses. The roadshows directly reach approximately 500 small businesses providing them with information security advice and guidance.

Get Safe Online was launched in October 2005. It is a national public and private sector initiative to raise awareness of internet safety amongst the general public and micro businesses (e.g.fewer than 10 employees or no employee with direct responsibility for IT security). Get Safe Online is supported by HM government, law enforcement and industry. More information available at www.getsafeonline.org

Get Safe Online's future plans include a campaign strategy to focus specifically on small to medium size businesses, in partnership with organisations such as Business Links and the National Computing Centre.

WARPs (see earlier). WARP members agree to work together in a community and share information to reduce the risk of their information systems being compromised and therefore reduce the risk to their organisation. This sharing community could be based on a business sector, geographic location, technology standards, risk grouping or whatever makes business sense.

Following on from a commitment in a UK Government White Paper, the DTI produced an online resource aimed at providing easy to understand guidance on information security for smaller businesses. This material has been added to and updated and is available at www.dti.gov.uk/sectors/infosec (the revised pages will be available from October 2006). A wide range of publications and other deliverables is available from this site. An online security health check tool based on the then British Standard BS 7799 (which has since become an international standard) has also been produced - this tool is at www.securityhealthcheck.dti.gov.uk

DTI acts as the Secretariat for the ISO 17799 UK Users' Group – an industry-led forum with the business mission of promoting and disseminating the exchange of good practice and know-how of good information security management based on the use of ISO 17799 and ISO

27001 (previously the British Standards BS 7799 Parts 1 & 2). The Group is led by a Steering Committee mainly consisting of industry representatives . Regular workshops and newsletters as well as networking opportunities are amongst the benefits of the (free) membership.

Internet Service Providers (ISPs)

Get Safe Online is working closely with the UK's ISP Association. A representative from GSOL will speak at the ISPA Annual Conference in September 2006 where there are plans to launch the availability of ISP 'auto-content' developed by Get Safe Online and available for use by all ISPs. BT, one of the UK's biggest ISPs, is a sponsor of Get Safe Online.

Media

It should be noted that the example listed below uses media as a channel to reach other target groups, and does not illustrate Media as a separate target group itself.

Get Safe Online has been the most significant sustained effort in achieving media coverage around internet security. The campaign was launched last October and in terms of media coverage to date, it has achieved the following:

- 208 items of coverage – 33 of these national broadcast and print – the rest were on local/regional radio and print
- Competition in free national newspaper (Metro – distributed in all major UK conurbations) – total reach of Metro competition: 18 million people. Metro competition entrants: 60,000 (double Metro's normal response rate of 29,000)
- "The Get Safe Online top-line entrant figures were the highest the group has ever had for a Metro competition. " Anthony Worssam, Head of Sponsorship & Promotions, Metro
- Steve Wright Show, Radio 2, 'Website of the Week'
- European Sabre PR/Media Award Finalist

In its launch week, the campaign reached 175,000 people directly – in person or visits to the website – delivering an equivalent cost 'per acquisition' of 60 pence (UK).

Although Get Safe Online has a budget of around £1 million in contributions from the sponsors, this is not enough to do a national above-the-line advertising campaign and a PR and online advertising campaign is the only viable option.

Plans are being developed for a further phase of activity starting in October 2006 using national, regional and local media.

Public-private partnership

Successful public-private partnerships (for awareness raising and education/training)

DTI works in partnership with various organisations in order to promote good information security practice. Examples of joint working over the past year or so include a joint guide with the Institute of Directors (available from the DTI website www.dti.gov.uk/sectors/infosec), a publication and a series of workshops about information security in the supply chain (a DTI/CBI/various private sector companies initiative). See www.cbi.org.uk

DTI has worked with Mid Yorkshire Chamber of Commerce to produce an e-learning package which is intended to be both easy and appealing to use. See www.bobs-business.co.uk

DTI is currently working with the Regional Development Agency (RDA) for Yorkshire (Yorkshire Forward), SOCA, local police forces within Yorkshire, and a local charity (People United Against Crime), to develop an information security web resource for the region, “Yorkshire Safe”. This will go live in October 2006 and will tie in with planned Get Safe Online promotional events. Contacts have been established with other RDAs and it is hoped further joint projects will materialise.

DTI has supported the development of the Institute of Information Security Professionals (IISP) www.instisp.org, designed to increase the professionalism and standing of information security professionals. The IISP was launched in February 2006 and within the first 3 months over 700 membership applications had been received including a number from overseas. Various Government departments including DTI, the Cabinet Office, CESG, NISCC have taken out corporate membership. DTI is currently working with IISP to develop a members’ web portal, this project should be completed by February-March 2007.

DTI works with industry to produce a biennial Information Security Breaches Survey. This Survey is the largest and most influential Survey of its kind and is entirely non self-selecting. The 2006 Survey was launched in April 2006, copies of the report are available from the ENISA website or see www.security-survey.gov.uk. The 2006 Survey was conducted for DTI by PricewaterhouseCoopers. A number of major security companies sponsored the work and various organisations (8 in all) acted as independent reviewers.

DTI is a member of various security-related organisations e.g. Information Security Forum (ISF – who acted as one of the independent reviewers for the 2006 Information Security Breaches Survey), Information Assurance Advisory Council (IAAC). For example DTI has hosted IAAC meetings including the IAAC Annual Symposium.

CSIA is a founder sponsor of Get Safe Online, a public/private sector joint initiative. Although it took some time to set up it is now producing a steady stream of awareness raising activities. The involvement of well-known UK and international brands such as BT, Dell, eBay, HSBC, Lloyds TSB and Microsoft has provided some extremely wide-reaching channels to internet consumers.

Some examples of corporate sponsor involvement in the initiatives

Microsoft provided online advertising and editorial throughout the launch month and GSOL took over their homepage on go-live day. This delivered over 60m impressions during October 2005 and had an equivalent advertising value of £200k. In addition to campaign activity, over 400 key words relating to security have been allocated by MSN on an ongoing basis.

Microsoft also led the launch regional roadshow programme featuring eye-catching branded Minis and online security advice in shopping centres delivered by hundreds of employee volunteers.

BT integrated GSOL activity with a wide range of issue related campaigns such as data on its Clean Feed service – a system that blocks search engine results for child pornography websites.

GSOL also featured heavily in a number of press releases, radio days and media relations activities covering ID fraud, online security and gaming. National press coverage has been secured via feature articles, and 3.25m security supplements fronted by Watchdog's Alice Beer were circulated with the Mail on Sunday in January. (Watchdog is a BBC TV consumer programme)

Additional ongoing support is provided via www.bt.com/security and their own Green Cross Code booklet.

HSBC are a frequent contributor to media comment as a GSOL spokesperson as well as active event speakers – such as the recent GSOL Executive Briefing held at Admiralty House and Guardian Unlimited podcast. HSBC has also undertaken a wide range of online promotional activities including prominent permanent links from www.hsbc.co.uk homepage and online banking customer direct mailings.

In addition to online promotion, LloydsTSB incorporated GSOL into their online banking security questionnaire and used ATM receipts to spread the message on 4m transactions during November. They also use GSOL content for their online security section.

The proactive nature of sponsor marketing has enabled GSOL to significantly extend its reach into areas that would be impossible to finance using a traditional marketing model. Advertising inventory on some of the UK’s most popular websites such as www.ebay.co.uk and www.paypal.co.uk has been secured and provides an excellent fit for shared objective – “to take control of your internet”.

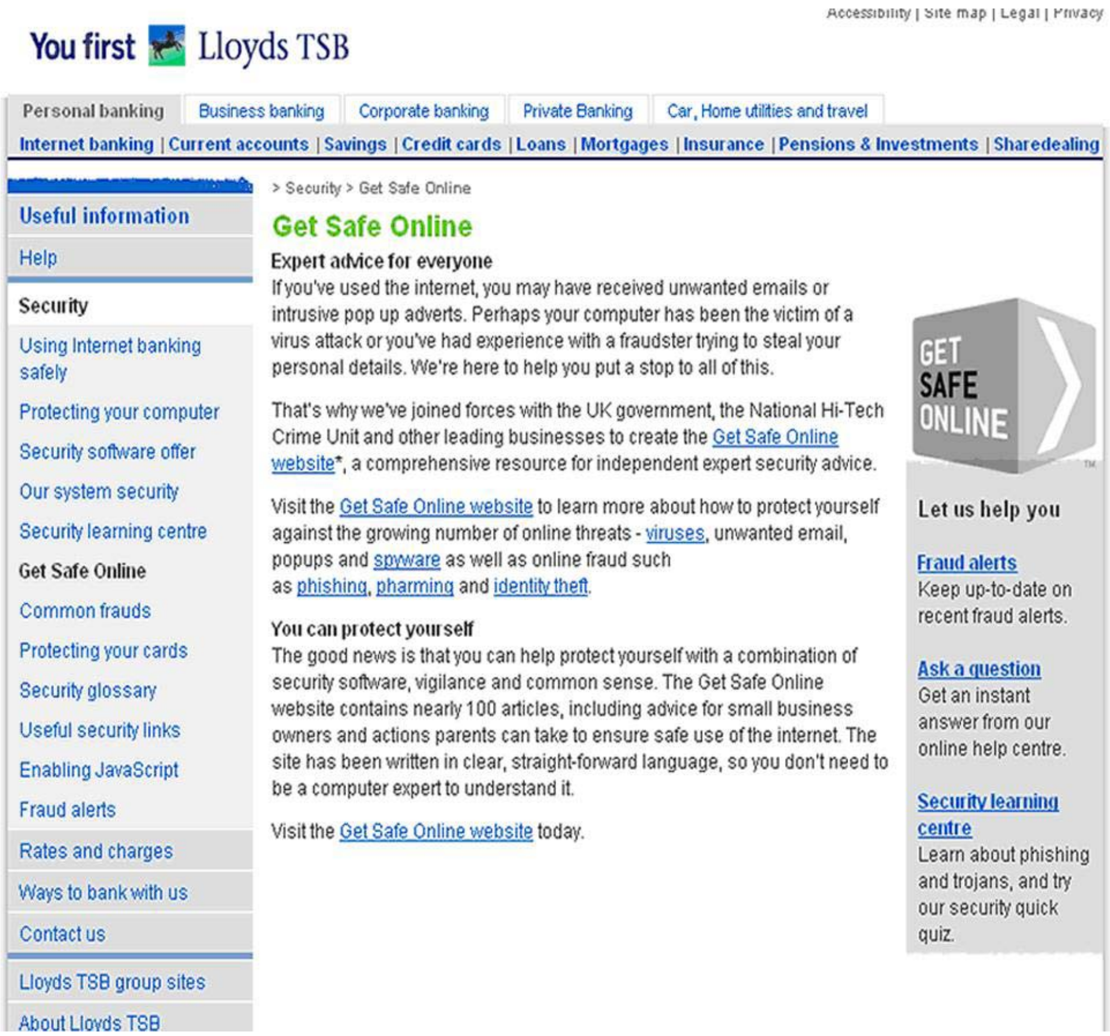
The value of this advertising space is over £200k and is perfect for GSOL – bringing the safety message front and centre at the exact moment when transactions are being made.

Support and coordination delivered by the Cabinet Office has underpinned GSOL’s initial set up and now provides key strategic input as well undertaking ‘business as usual’ functions. Ministerial support and active government endorsement is integral to the impact of GSOL and has enabled aligned working with a number of the UK’s largest not-for-profit organisations as well as Directgov. These include Business Links, Citizens Advice and UK Online.

The new Serious Organised Crime Agency (which took over the functions of the National Hi Tech Crime Unit as well as various other organisations) have been active supporters and continue to chair the GSOL Steering Group for the 2006-2007 period.

The role of supporting organisations has been very helpful in spreading the message with in-kind support such as joint press releases with ABTA (Association of British Travel Agents) and business breakfasts for British Chambers of Commerce members. GSOL will continue to work with membership and consumer organisations during the next twelve months in order to target its audience messages more efficiently and effectively.

An example of sponsor activity



Get Safe Online

Expert advice for everyone

If you've used the internet, you may have received unwanted emails or intrusive pop up adverts. Perhaps your computer has been the victim of a virus attack or you've had experience with a fraudster trying to steal your personal details. We're here to help you put a stop to all of this.

That's why we've joined forces with the UK government, the National Hi-Tech Crime Unit and other leading businesses to create the Get Safe Online website*, a comprehensive resource for independent expert security advice.

Visit the Get Safe Online website to learn more about how to protect yourself against the growing number of online threats - viruses, unwanted email, popups and spyware as well as online fraud such as phishing, pharming and identity theft.

You can protect yourself

The good news is that you can help protect yourself with a combination of security software, vigilance and common sense. The Get Safe Online website contains nearly 100 articles, including advice for small business owners and actions parents can take to ensure safe use of the internet. The site has been written in clear, straight-forward language, so you don't need to be a computer expert to understand it.

Visit the Get Safe Online website today.

Let us help you

Fraud alerts
Keep up-to-date on recent fraud alerts.

Ask a question
Get an instant answer from our online help centre.

Security learning centre
Learn about phishing and trojans, and try our security quick quiz.

Government as partner with civil society

Recent awareness programmes and initiatives

Refer to the *Gov. as Developer* and *Gov. as Partner (Business)* sections for information on the Get Safe Online campaign. The campaign is also targeted at the Home User group.

Metrics and key performance indicators (KPIs)

Metrics/KPIs for assessing the success of an awareness raising initiative

The following metrics have been used to measure the effectiveness and impact of the Get Safe Online marketing, public relations and brand building during 2005-2006, and it is anticipated that these will continue into the new financial year starting July 2006.

- Qualitative and quantitative market research on behaviour change
- Opportunities to see across print and broadcast media
- Web site traffic trends, including third party content usage
- Third party website links to GSOL
- Participation by partner organisations in promotional activities

Performance and Impact Summary

Launch Period October - December 2005. Control group of 500 respondents - Total survey pool of 1617.

33% of respondents were aware of the campaign or logo within one month of go-live, of this group:

- 62% recognised the need to be careful when being online
- 52% recognised it was their responsibility to stay safe
- 52% understood the potential risks
- 40% said that they had been prompted to find out more

Awareness of threats such as key-logging and phishing rose by 15pts and 12pts respectively Behaviour change had the greatest impact on backing-up data 75% vs. 53% for the non-aware

Post campaign respondents were:

- More likely to have installed a firewall or anti-spy software
- Significantly more likely to back up their data
- Significantly more likely to keep personal details private
- More likely to use and update anti-virus and anti-spyware tools regularly

Contra-Indicators

19% of respondents felt less secure once aware of the risks whilst 24% felt more secure through increased knowledge and reassurance that they were doing the right thing

Web Site Traffic and Performance

During the launch phase 114 000 visitors were recorded on the site, and all successive marketing and public relations activity shows a clear and consistent correlation to web traffic generation. It is anticipated that baseline visitor numbers will have reached c500k before October 2006 – a significant achievement for a non-product or service related start-up promotion within a twelve month period.

At the present time, the annualised visitor run-rate stands at 282 000 before any significant marketing activity is undertaken. This figure is planned to rise ten-fold through further enhancements such as search engine optimisation and sponsor site background promotional activity.

www.getsafeonline.org is featured on over 13000 active web pages which link directly back to the site, this compares very favourably with alternative information providers:

- 450 to www.banksafeonline.org
- 260 to www.besafeonline.org
- 92 to www.staysafeonline.org

Campaign Initiatives

Wales E-Crime Awareness Programme

Through the E-Crime Summit in Wales, the Welsh Assembly Government, the four Welsh Police forces, the Welsh Development Agency, Morgan Cole, and the National High-Tech Crime Unit are demonstrating a commitment to a programme of education, investment and support that will encourage a new generation of companies to build secure and crime-resistant foundations for the economic future of Wales.

e-Crime Summit

More than 200 delegates from a range of businesses and organisations participated in this years 2006 Summit. The Summit delivered a manifesto, outlined a proposed three- year Action Plan to protect organisations from on-line crime and mapped out the practical steps needs to ensure the success of this action plan amongst the responsible bodies.

By attending, delegates received up-to-date briefings and insights from senior representatives of Microsoft, the National Hi-Tech Crime Unit, Morgan Cole Solicitors and HSBC on the scale and nature of this very real threat to businesses.

More importantly delegates learnt how the Manifesto proposes to support and protect Wales against cyber crimes through a package of quality advice, awareness raising, information's sharing, staff training, tighter procedures and vigilance.

For more information on the summit, refer to:
http://www.wda.co.uk/index.cfm/technology_and_innovation/mtp/partner_programme/ecrime/en8118

Refer to http://www.wda.co.uk/resources/E-Crime_Wales_Manifesto_Final2.pdf for a copy of the summit manifesto.

Refer to e-crime_wales_action_plan_final2.pdf for a copy of the Action Plan

SaferInternet - Internet Safety Zone (article)[26]

Summary

[26] http://www.saferInternet.org/ww/en/pub/insafe/news/articles/0706/uk1.htm, 1st August 2006.

The InternetSafetyZone.com portal is a one-stop-shop for disseminating holistic Internet safety advice to parents, educators and children. It has been in development for over a year at the Cyberspace Research Unit, University of Central Lancashire (UCLAN) - the EU's UK node, and co-ordinating partner on the ISCA project.

Details

Internet Safety Zone (ISZ) offers a wealth of information on a variety of topics such as: how the Internet works, e-mail, chat, instant messaging and social networking. These topics are covered from a technical perspective (how e-mail is created, delivered and received for example) but also from an Internet safety perspective (e.g., what are the potential dangers to children using chat rooms?). Users can browse through general to more in-depth information.

In addition, ISZ also aims to provide a more holistic approach to Internet safety by covering topics within what is termed 'cyberwellness.' Issues such as racism, human rights, self-harm, suicide and eating disorders are covered in detail. Children are encouraged to gain critical awareness when using the Internet and realise that not everything they see online will be 'the truth'.

The content for ISZ has been gathered and written in conjunction with a wide variety of organisations in order to develop best practice. Indeed, many organisations such as AOL, BBC, Becta, Childnet, ELSPA, Internet Watch Foundation (IWF), Microsoft, NSPCC, O2, Vodafone, police forces and the Virtual Global Taskforce (VGT) have helped to provide sound advice and guidance for parents and children alike in using web and mobile communications technologies.

ISZ has also listened to criticisms levelled at many EU node portal websites by encouraging a straightforward and clear pathway to reporting Internet safety issues. From the homepage itself users can, with but one-click, go to pages with relevant information and links to organisation where they can make a report. An example is the "report abuse icon" for child abuse images that takes users to a page clearly indicating that they can make a report to the IWF and how to do so.

Moreover, ISZ also offers information for individuals or groups to receive directly to their PC as new content becomes available. Each topic has an RSS link that allows a user or organisation to make use of the content in an open and flexible manner: individuals can receive updates directly to their inbox/RSS aggregator, and organisations can display the latest information on their own websites/portals through incorporating an RSS 'window' on their website.

This is a key aspect of ISZ; to allow other organisations to be able to disseminate Internet safety advice quickly and simply to those who might not ordinarily be exposed to the topic. Furthermore, this allows ISZ, and through it the topic of child Internet safety, to reach a far wider audience.

Refer to http://www.Internetsafetyzone.co.uk, to visit the Internet Safety Zone

Good Practices by Target Group

Home User

Current Situation

The Home User target group is heavily targeted in most information security awareness raising initiatives within the Member States. The main audience tends to be the Young or Adults – Silver Surfers are targeted less. A variety of communication channels are used to convey awareness messages, with portals, public events, comics and the use of media (e.g. TV) being among the most popular mediums used.

Country Good Practices

Austria

The SaferInternet.at initiative is currently focusing on parents as a main target group for improving safety of the Internet and mobile use by minors. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Austria

Belgium

In Belgium, when children reach the age of 12, they receive an electronic ID with a comic telling the story of security awareness. They also get an electronic card reader that will allow them to chat safely on certain pre-defined websites. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Belgium

A fictitious website for a Mobile Phone operator proposes free subscriptions to services such as mobile phones, SMS and email. Mainly targeted at the youth, to register, the surfer must submit personal data. The site displays a message that the operator does not exist, and takes the surfer to another site with details on information security. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Belgium

Denmark

The annual Net-safe now! campaign is aimed at creating awareness about IT security and to promote safer behaviour on the Internet. Targeted at multiple groups, the campaign is done in cooperation with multiple partners and uses various channels in which to convey messages. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Denmark

For more information on awareness raising initiatives such as the “Youth Ring”, a collaboration between after school centres and youth clubs, click on the following link to go to the details in the *Good Practices by Country* section for Denmark

Finland

A Guide for the safer Internet at home (Joka Kodin Tietoturvaopas) was distributed to over 1 million homes in Finland. The initiative was complemented by a website. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Finland

Also in Finland, the *Hiiripiiri* handbook (circulated to school children as part of the curriculum, with certification available), the Safer Internet Day, the comic books for children as well as the collaboration with content providers are all awareness raising initiatives. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Finland

France

As part of an initiative to raise awareness for the Young, the French Ministry along with partners from business and society including ISPs, have launched a multi-channel campaign including the use of TV short films. For more information, click on the following link to go to the details in the *Good Practices by Country* section for France

Germany

The Federal Government targets people at all levels in an effort to raise awareness. Various materials and tools inform and support non-professional users. Private users can also sign up for alert services. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Germany

Greece

As part of the Insafe node, the SafeNetHome initiative is meant to be a hard-hitting campaign raising awareness across target groups but especially with the kids and youngsters. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Greece

Hungary

There have been initiatives by the Government and civil societies in undertaking several collaborations in the field of awareness raising for the protection of Home Users and the general public (including SMEs). For more information, click on the following link to go to the details in the *Good Practices by Country* section for Hungary

Iceland

The SAFT project, primarily aimed at the youth but also targeting parents as a channel to communicate with the Young, has undertaken awareness work on several fronts. A variety of channels have been used including brochures, surveys, animated advertisements, newspaper articles, blogathans and conferences. A range of media outlets have been used for the campaigns, covering issues such as mobile phone safety, computer games and safe and ethical use of the Internet. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Iceland

Italy

A project initially targeted at Adults, aims to fill the gap between citizens and new technologies documented in other ongoing projects. The contents of the project will be organised as an educational course, freely accessible from institutional organisation web portals. Also, there are plans to raise awareness within SMEs through seminars, web based e-learning and through media such as TV. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Italy

Lithuania

A number of initiatives to raise awareness in the general public have already been run or are planned. These include using forums for discussions, articles, tools and brochures. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Lithuania

Luxembourg

Various initiatives have been and continue to be undertaken with the aim to raising awareness amongst citizens. Specific messages are communicated to this target group using various channels including flash movies, portals and road shows. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Luxembourg

Malta

Various initiatives have been undertaken targeting children, parents and the elderly. These have mainly been in the form of surveys, courses and publications. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Malta

Netherlands

Various initiatives have been undertaken targeting the Home User. Channels used include fairs, websites, knowledge sharing events, materials such as brochures and public events. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Netherlands

Norway

A public-private initiative including ISPs has seen the creation of a website aimed at the general public. The website provides information, advice and guidance for secure and safe use of the Internet. The content is grouped into themes and categories. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Norway

Poland

Several projects under the responsibility of the Ministry and with collaboration from other bodies are aimed at the Home User and SME target groups. The main channels used have included websites, a Hotline and public events. ISPs have also been collaborated with on addressing certain IT security issues. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Poland

Portugal

Several initiatives have been undertaken or are underway aimed at raising awareness in the Home User, ISP and Local Government target groups. These have mainly been undertaken through training, public events or collaboration. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for Portugal

Slovenia

The main initiatives have focused on raising awareness among the Home User target group (particularly the Young). Several channels have been used including websites, training sessions, public events and a hotline. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Slovenia

Sweden

Sweden has conducted or is still conducting various awareness raising initiatives aimed at the Home User, SME and Local Government target groups. Some examples include a project run by the National Post and Telecom Agency which uses interactive websites and publications among other channels, as well as the SurfaLugnt project which has been created with collaboration from the IT industry and relevant authorities. Another initiative, by the City of Stockholm, has seen the creation of a film based on the roles of public sector employees for public sector employees, also covering security guidelines. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for Sweden

Regional seminars are also being conducted in an effort to disseminate knowledge of safer Internet use. These seminars are mainly targeted at teachers but also include other professionals working with children. One of the more successful elements is the use of youth panels to show how young people use and perceive new media. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Sweden

United Kingdom

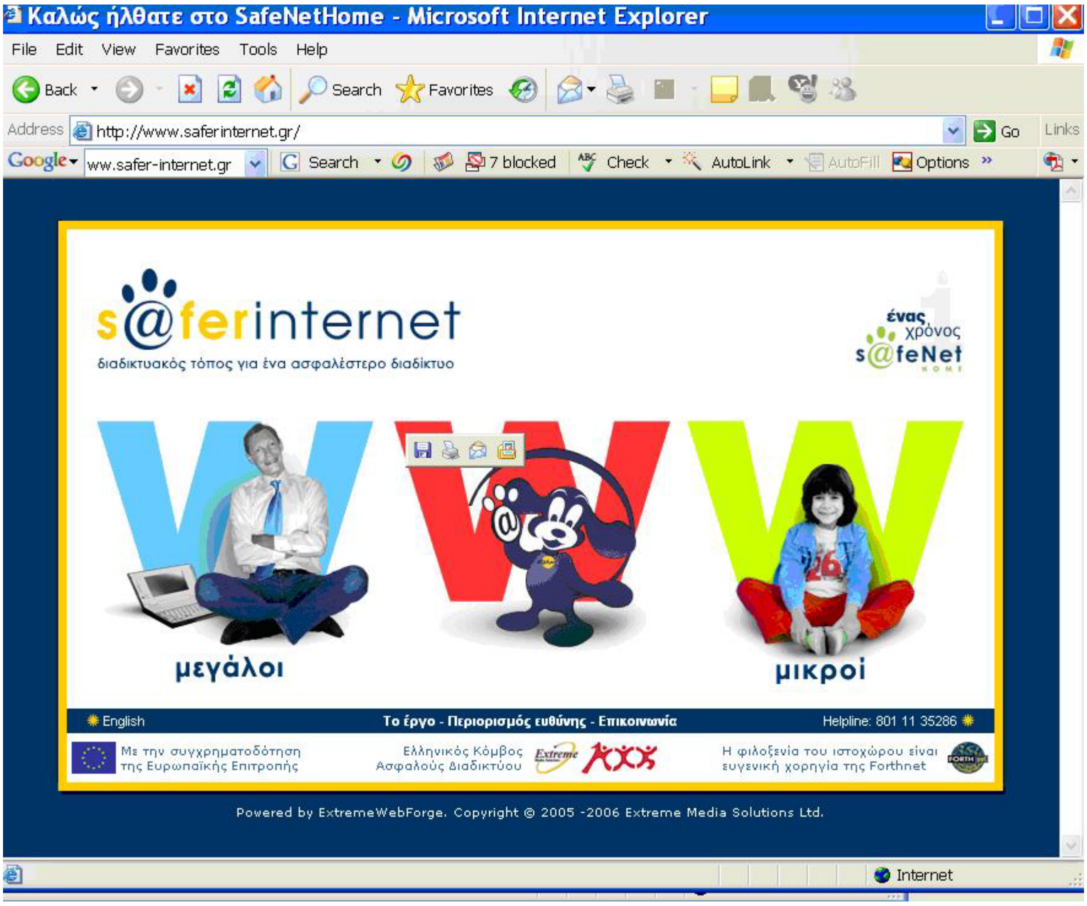
Several awareness raising initiatives have been aimed at the Home User, SME and Local Government target groups. Channels used for delivering awareness messages have included websites, public events, national media (such as TV and radio) and road shows for the public sector. Development programmes such as CSIA also aim to raise national and local cross-Government awareness. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for United Kingdom

The InternetSafetyZone.com portal is a one-stop-shop for disseminating holistic Internet safety advice to citizens. The content is gathered and written in conjunction with a variety of organisations. The site has easy navigation and easy to use functionality to report incidences. For more information, click on the following link to go to the details in the *Good Practices by Country* section for United Kingdom

Other Organisation Good Practices

FORTH

Over the past several years, EKATO (http://www.ekato.gr) has been leading a Greek nation-wide project on the awareness for Internet safety. A screenshot of the web portal developed can be viewed below. For more information, refer to www.saferInternet.gr



Καλώς ήλθατε στο SafeNetHome - Microsoft Internet Explorer

http://www.saferinternet.gr/

ww.safer-internet.gr

διαδικτυακός τόπος για ένα ασφαλέστερο διαδίκτυο

English   Το έργο - Περιορισμός ευθύνης - Επικοινωνία   Helpline: 801 11 35286

Με την συγχρηματοδότηση
της Ευρωπαϊκής Επιτροπής

Ελληνικός Κόμβος
Ασφαλούς Διαδικτύου

Η φιλοξενία του ιστοχώρου είναι
ευγενική χορηγία της Forthnet

Powered by ExtremeWebForge. Copyright © 2005 -2006 Extreme Media Solutions Ltd.

US National Cyber Security Awareness Month 2005

For the second year in a row, the public and private sector joined forces to organise National Cyber Security Awareness Month, a national collaborative effort to educate Internet users of all ages about safe online practices. The National Cyber Security Alliance (NCSA) is pleased to report that National Cyber Security Awareness Month, 2005 was a solid success. Through a combination of media relations and state and local events, we estimate that we reached more than 70 million consumers with NCSA messages throughout the month of October. As a result of these media events, traffic to the NCSA website increased by over 300% from September to October, culminating in a total of 114,992 visits to the website in October – an increase of 14% over the goal of attracting 100,000 users to the site for the month, and the largest number of visits in a single month to staysafeonline.org to date.

The summary results noted above are demonstrable progress against our objectives for the month, specifically:

- To increase awareness of computer security issues and the National Cyber Security Alliance across designated key audiences – Home Users, SMEs and the education community
- To encourage the adoption of safe online behaviours among key audiences during National Cyber Security Awareness month, and beyond

To achieve results against the above-stated goals, the NCSA and our partners embarked upon a multi-faceted consumer education campaign, which comprised the following elements:

- A media relations campaign highlighting National Cyber Security Awareness Month, which emphasized TV coverage as a means by which to create a “domino effect” of media momentum which would trickle down to all target audiences during October
- A television PSA, which would augment media relations efforts and provide an additional layer of awareness for NCSA
- Multiple state and local-market events, which provided a grassroots forum for explaining computer security issues and educating the public about safe online behaviours
- All activities culminated in a call-to-action to visit www.staysafeonline.org for more information, including tips for maximizing online security. To ensure a positive consumer experience, the website was re-designed for greater-ease-of-use, visual appeal and comprehensiveness, including providing links to additional sites beyond NCSA

The results for National Cyber Security Awareness Month were indeed impressive, and certainly represent a marked improvement over those attained in the inaugural year of 2004. Nonetheless, there are many ways in which we can improve our efforts for 2006. Preliminary recommendations include:

- *Secure approval of all stakeholders and grassroots events early.* Although a plan for NCSAM was submitted in July, three weeks before October began, there were still discussions and decisions being made regarding spokespeople, pitch strategy, etc. Each new wave of deliberations required many participants and cost valuable pitch time, ultimately delaying the satellite media tour, a key component of NCSAM. Additionally, many local market/grassroots events were still being finalized (or in some cases, cancelled) as of mid-September causing ambiguity about the scope and level of PR resources to be devoted to those activities. Ultimately, everything worked out, but our hope for next year is to have all stakeholders be part of the planning and approval process, so that an approved plan is ready for execution by mid-August, and there are minimal late-stage strategy revisions

- *Craft a more compelling message.* The biggest challenge facing the NCSA is that computer security is covered frequently in the media, and the end-result is usually disparate entities all giving variations on tips about using anti-virus software, firewalls, etc. Although this year's campaign focusing on identity theft generated good results, we feel we could have accomplished more, and secured national media coverage with a fresh and new bold approach. We understand that particular campaign may never generate consensus among all NCSA stakeholders, but we hope next year to execute a campaign that will take more risks and have a point-of-view that is unique to NCSA
- *Have necessary media tools in place and/or be able to respond quickly to opportunistic media opportunities.* Although a worthy cause, the reality is National Cyber Security Awareness Month is a manufactured news event -- *not news in and of itself*. Therefore, it is critical to release new information in the form of a study during NCSAM, or sponsor a program that is news worthy

Refer to us_national_cyber_security_awareness_month_2005_summary_2.pdf in the *Reference Files* section for more information on this US campaign.

SME

Current Situation

The SME target group is often targeted in awareness raising initiatives within the Member States, however priorities seem to be to the Home User. The main SME audience targeted tends to be the standard employees; however messages are applicable to the other SME categories. The popular channels used include training, seminars and online resources.

A survey by Trend Micro, a leader in antivirus and content security, has found that some end users in enterprise environments around the world are more likely to engage in riskier online behaviour at work than home.[27]

- The study, conducted in July 2005, featured more than 1,200 corporate end users in the United States, Germany, and Japan who responded to an online survey. Of the many findings, perhaps the most significant is the correlation between the presence of an IT department and end user confidence in the security they expect against viruses, worms, spyware, spam, phishing and pharming (these expectations often result in riskier online behaviour that exacerbates IT's challenge to protect business operations from increasingly unpredictable threats)
- Of those who responded, 39% of enterprise end users believed that IT could prevent them from falling victim to threats like spyware and phishing. This belief prompted many of them to admit bolder online behaviour. Of those who admitted to engaging in bolder online behaviour, 63% acknowledged that they are more comfortable clicking on suspicious links or visiting suspicious websites because IT has installed security software on their computers. 40% of those who admitted to engaging in riskier online behaviour said it was because IT was available to provide support if problems occurred

[27] http://www.trendmicro.com/en/about/news/pr/archive/2005/pr091305.htm

Country Good Practices

Austria

The IT-Safe initiative focused on smaller businesses, particularly SMEs with up to 25 employees and offers specific advice depending on the level of knowledge and IT infrastructure. An organisation specific handbook is created, with supporting software from various security companies. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Austria

Czech Republic

An initiative between the Ministry and Microsoft has targeted SMEs in an effort to promote information security. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Czech Republic

Denmark

The annual Net-safe now! campaign is aimed at creating awareness about IT security and to promote safer behaviour on the Internet. Targeted at multiple groups, the campaign is done in cooperation with multiple partners and uses various channels in which to convey messages. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Denmark

Finland

As part of the National Information Security Day 2006 Project, an online service was launched aimed at SMEs, providing a comprehensive picture of information security. The online service functions as a guide and it is especially targeted at both employers and employees. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Finland

Germany

The Federal Government targets people at all levels in an effort to raise awareness. Portals exist for professionals with security manuals and guidelines as well as other security information. Large public-private partnerships exist with various organisations. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Germany

Hungary

There have been initiatives by the Government and civil societies in undertaking several collaborations in the field of awareness raising for the protection of Home Users and the general public (including SMEs). For more information, click on the following link to go to the details in the *Good Practices by Country* section for Hungary

Ireland

VigiTrust, a private organisation, specialises in awareness raising training for both the public and private sectors. Refer to details in the *Good Practices by Target Group, Other Organisation Good Practices* section for Local Government.

Italy

A project initially targeted at Adults, aims to fill the gap between citizens and new technologies documented in other ongoing projects. The contents of the project will be organised as an educational course, freely accessible from institutional organisation web portals. Also, there are plans to raise awareness within SMEs through seminars, web based e-learning and through media such as TV. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Italy

Lithuania

A number of initiatives to raise awareness in the general public have already been run or are planned. These include using forums for discussions, articles, tools and brochures. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Lithuania

Luxembourg

Various initiatives have been and continue to be undertaken with the aim to raising awareness amongst SMEs. Specific messages are communicated to the target group using various channels including flash movies, portals and road shows. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Luxembourg

Malta

Various training courses are being created on how businesses can use ICTs. Topics covered include awareness raising. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Malta

Netherlands

Awareness raising initiatives undertaken include surveys and training programmes. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Netherlands

Norway

A public-private initiative including ISPs has seen the creation of a website aimed at SMEs. The website provides information, advice and guidance for secure and safe use of the Internet. The content is grouped into themes and categories. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Norway

Poland

Several projects under the responsibility of the Ministry and with collaboration from other bodies are aimed at the Home User and SME target groups. The main channels used have included websites, a Hotline and public events. ISPs have also been collaborated with on addressing certain IT security issues. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Poland

Sweden

Sweden has conducted or is still conducting various awareness raising initiatives aimed at the Home User, SME and Local Government target groups. Some examples include a project run by the National Post and Telecom Agency which uses interactive websites and publications among other channels, as well as the SurfaLugnt project which has been created with collaboration from the IT industry and relevant authorities. Another initiative, by the City of Stockholm, has seen the creation of a film based on the roles of public sector employees for public sector employees, also covering security guidelines. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for Sweden

United Kingdom

Several awareness raising initiatives have been aimed at the Home User, SME and Local Government target groups. Channels used for delivering awareness messages have included websites, public events, national media (such as TV and radio) and road shows for the public sector. Development programmes such as CSIA also aim to raise national and local cross-Government awareness. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for United Kingdom

Through the E-Crime Summit in Wales, the Welsh Assembly Government and other organisations have committed to a programme of education, investment and support that encourages SMEs to build secure and crime-resistant foundations. For more information, click on the following link to go to the details in the *Good Practices by Country* section for United Kingdom

Other Organisation Good Practices

FORTH

The e-Business Forum (http://www.ebusinessforum.gr/) organises dissemination activities for business-related security practices including digital payment, digital signatures and digital authentication methods.

Go-online.gr (http://www.go-online.gr) provides SMEs and individual professionals with information on network security and privacy.

The National Documentation Center (http://www.ekt.gr) frequently organises events in order to inform the Greek Scientific and Industrial Community about funding and collaboration opportunities which may exist in the context of European programs.

Public-private partnerships

MD5 (http://www.md5sa.com) and ENCODE (http://www.encode.gr) frequently organise awareness events on security.

Metrics and KPIs

Safeline (http://www.safeline.gr), the first Greek Hotline for the safer Internet access, performs periodic assessments of its activities based on performance indicators used by Hotlines all over Europe. These performance indicators include, but are not limited to, accessibility, visibility, relationship with law enforcement agencies and cooperation with other Hotlines. The full list of performance indicators can be made available if requested.

Developing common metrics is important. Once such metrics will have been developed, they should be communicated to the Member States with the recommendation to apply them in their future events, in order to measure a campaign's success and calibrate one State's results against the results of other States.

SAP

Effective awareness raising initiatives

Mcert was founded by the membership association BITKOM, the Federal Ministry of the Interior, the Federal Office for Information Security, and several qualified industry partners as a public-private partnership. Based on objectivity and manufacturer independence, Mcert provides IT security expertise, which is mainly directed at small and medium-sized businesses. Providing trustworthy and reliable knowledge, Mcert supports SMEs in solving security issues. Customers benefit from security advisories and recommendations for service providers. For more information, refer to http://www.mcert.de/

Bürger-CERT informs and advises the public about topical security issues. Started in March 2006 as an ongoing project, the services are completely objective and free of charge. The intention behind Bürger-CERT is to make the general public aware of omnipresent threats on the Internet and electronic communication systems. Users can register to receive relevant information via e-mail. Bürger-CERT is a common project of the Federal Ministry of the Interior and Mcert German Association for IT-Security. For more information, refer to http://www.buerger-cert.de/

Deutschland sicher im Netz (DsiN) Initiative

A project by the German Minister for Economic Affairs and Employment and the Federal Ministry of the Interior, "Mittelstand sicher im Internet", provides a website with information for small and medium-sized businesses. Its goal is to raise awareness, show risks, and provide simple and efficient solutions. The initiative maintains a close cooperation with the private sector: Bitkom e.V., Bundesverband der Deutschen Industrie e.V. (BDI), the German Chamber of Commerce (DIHK), Mcert, TeleTrusT Deutschland e.V. and other associations. For more information, refer to http://www.mittelstand-sicher-im-Internet.de/

Companies like eBay and T-Online have joined ranks with SAP and Microsoft in the initiative, supported by the German Minister for Economic Affairs and Employment. A total of 14 alliance partners have committed themselves to increased security in developing electronic business processes, greater reliability in developing and operating software, and data protection. The participants will support the initiative with immediate information campaigns, guidelines, and software tools that increase company and consumer security and confidence. Results have been reviewed in May 2006. For more information, refer to https://www.sicher-im-netz.de

The initiative is based on seven pledges for action:

- Microsoft and Computer Associates are to develop and distribute a security check that shows gaps in the system
- eBay is to make a learning package available that informs users about the legalities and risks of secure online business
- Microsoft, German children's assistance organisation Deutsches Kinderhilfswerk, and a group of volunteers for multimedia service providers are to create an Internet portal for children aged 8-13, to train them on media skills
- SAP, Mcert and Microsoft will supply small and midsize businesses with a package for information security
- Teletrust and German publishing company Deutsche Sparkassenverlag are to provide information, trainings, and certificates for encryption technology for small and midsize companies and system resellers
- SAP and Microsoft are to commit themselves to secure development and provide universities with information to ensure students learn about security risks and how to avoid them in software development
- T-Online is to provide a free "security barometer" that enables every user to determine the security risk of electronic transactions

SME definition

The ENISA definition of what constitutes an SME is typically adopted, however between 250 and 5000 employees would be a better fit for defining Medium enterprises.

Main issues of target group

SMEs use e-commerce and the Internet in their daily business, but they do not have the financial and personnel resources to handle the security aspects of electronic communications. They have to protect their success. Business owners or managers are seldom aware of the legal liabilities connected with IT security. ICT specialists need assistance with security issues, and employees need to be aware of threats and dangers.

Target audience description

The audience consists mainly of ICT specialists with a low level of knowledge. Some Initiatives also address employees, directors or managers all with either a low level of or without knowledge/awareness.

Channels used

The Internet is the main communication channel. In addition, some initiatives raise awareness through either CD-ROMs or through local events.

For the DsiN initiative, there was a start (kick-off) event. The following communication channels were used: website, press conferences, CD-ROMs, books, radio broadcasts, TV and truck tours.

Use of multipliers

The DsiN initiative used university programs as a multiplier factor. By using the university networks of SAP and Microsoft, the initiative reached 60,000 students with its secure programming awareness sessions.

Timeframe

The initiative is for a minimum of 1 year in length.

Lessons learnt

DsiN was a perfect private-public partnership. Driven mostly by the industry, it was a great combination of real help for the target groups and image/PR for the members of the initiative. However, even though the budget was very high and the media reported regularly about DsiN, the level of awareness among the target groups is still not sufficient. IT-security initiatives are like any other marketing campaign: if you want to achieve a "brand recognition” of 80% you need a sufficient budget and constant penetration.

Metrics/KPIs

Example of the metrics/KPIs used in the “Deutschland sicher im Netz” initative:

- Web statistics
- Number of people attending events
- Number of training provided by certified “Deutschland sicher im Netz” partners
- Number of visitors at DsiN booths at trade shows (Systems, Cebit)

The assessment of the initiative is ongoing. Parallels may be drawn to product marketing or any other image campaign. Every part of the awareness campaign has to be measured and controlled to see which actions lead to success and to stop ineffective parts of the campaign.

Swiss Re

Swiss Re is one of the world's leading reinsurers and the world's largest life and health reinsurer. With 70 offices in some 30 countries, the company has 10,000 employees.

The project: challenges and issues

Swiss Re has recently executed an awareness raising campaign as the company takes security seriously and understands that there has been a substantial increase in IT security-related risks and threats. Having strong technical protective measures in place, the company realises that the infrastructure and efforts to date will be useless if staff are not aware of the risks to IT security and do not act accordingly. This "human factor" is a critical component of information security within an organisation. Awareness is considered to be part of the security strategy of the company.

A project team was established. People of different departments (e.g. legal, business groups etc) were invited to be part of the team. A series of initial investigative studies were carried out. These included target audience analysis, cultural bias analysis, IT security perception reviews, management interviews and an analysis of awareness techniques. As part of the analysis:

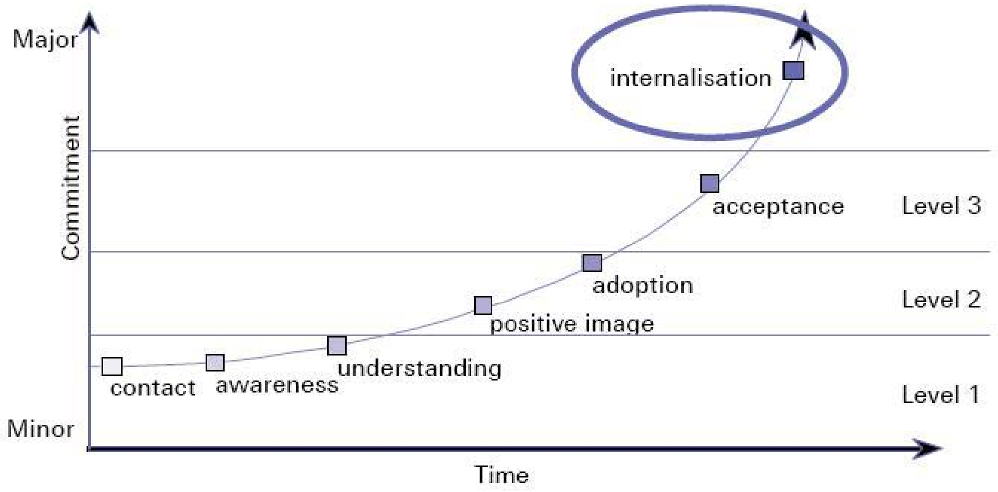
- 3 target groups were identified: Managers, End Users and IT Staff
- 2 types of employees were identified: Individualists (who take on responsibility) and Hierarchists (those averse to taking risk)
- The reviews showed that information alone was not enough to bring about the change in behaviour being targeted
- Active support of senior management was seen as crucial for the success of any awareness raising initiative

Several observations were noted as being important when running an awareness raising campaign. Initiatives should:

- Be aware of cultural and languages differences and be tailored accordingly
- Maximise the use of existing communication channels
- Be sensitive to information overflow
- Be group-wide in scope, but targeted at individual audiences

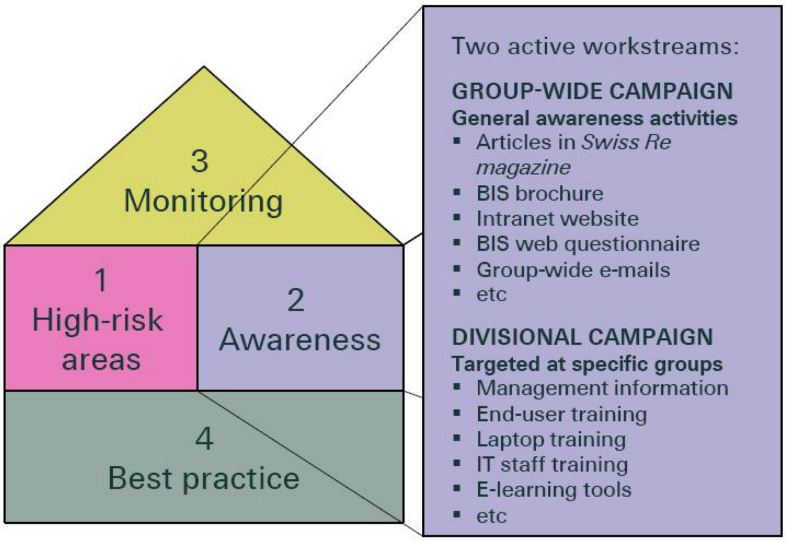
The approach: two workstreams

The goal of the awareness raising campaign was to change the employee's attitudes over the long term (resulting in internalisation):



Source: ING Group, Amsterdam

The campaign was executed across two workstreams: a group-wide campaign consisting of general awareness activities and a divisional campaign, which targeted specific user groups. A top-down approach has been used for this workstream. Different techniques and media were used for each of the workstreams:



Two active workstreams:

GROUP-WIDE CAMPAIGN

General awareness activities

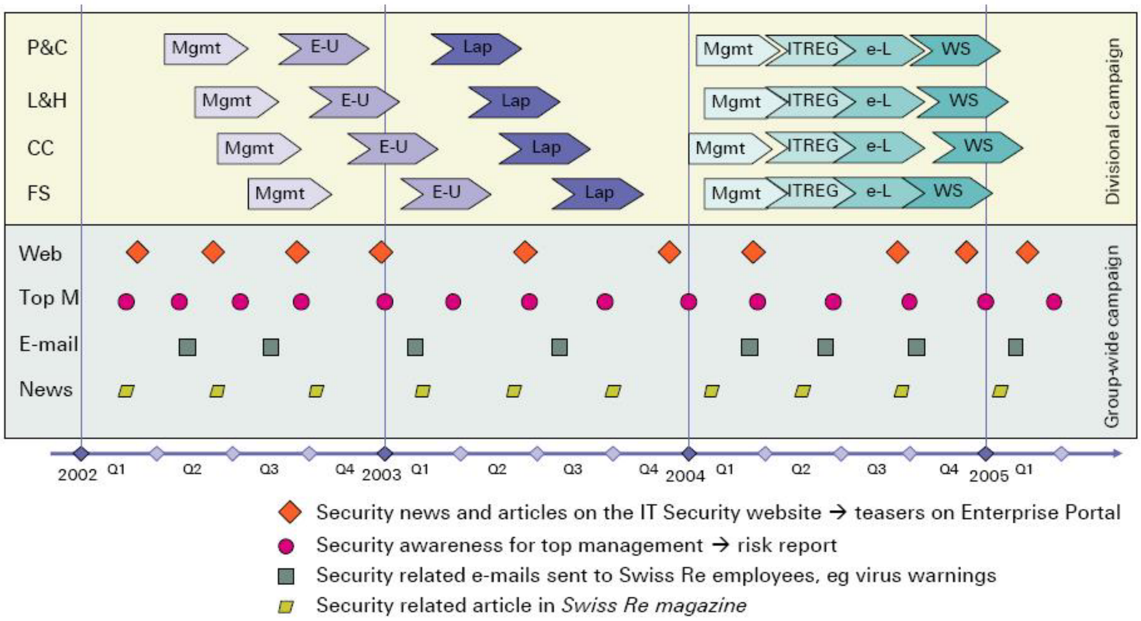
- Articles in *Swiss Re magazine*
- BIS brochure
- Intranet website
- BIS web questionnaire
- Group-wide e-mails
- etc

DIVISIONAL CAMPAIGN

Targeted at specific groups

- Management information
- End-user training
- Laptop training
- IT staff training
- E-learning tools
- etc

A high-level rollout plan was constructed detailing the main activities of the divisional campaign (across the different businesses and user groups) and the group-wide campaign (using different media):



Take it to the users: kick-off

When the campaign was started, several activities were undertaken:

- A movie was shown to the Swiss Re top management. The movie highlighted important risks such as the use of simple passwords and sending confidential information by fax
- A week later, articles about Business Information Security were written in the company magazine. “Do’s and Don’ts” paper wrappers were put around the magazines, forcing employees to read the wrapper before accessing the magazine. Also, entering the password given inside of the wrapper on the new IT security website would make the employee eligible for winning a prize
- A new IT security portal dedicated to security matters was launched. This allowed for one face to the customer

Classroom-based training sessions

Before commencing the classroom-based training sessions, training material was prepared. This included slides, handouts, teacher’s guides, printed material (such as cards) and trainer’s toolboxes. Material was produced in English and then translated into 4 languages: German, French, Italian and Spanish). Feedback rounds and review workshops were conducted as well as “Train the Trainer” sessions. These sessions were run by professionals and included topics on how to hold workshops and how to motivate participants. To test the training structure and format, a pilot was run in two locations. As part of the classroom-based training:

- Three topics were presented during the sessions: email risks, Internet risks and password risks
- Interactive workshops allowed for discussions, case study analysis, video, theory and questions and answers (Q&A) sessions
- End user and laptop sessions were mandatory
- Over 700 sessions took place
- Participants were asked to complete feedback forms which helped create a "before and after" picture. Nine different questions on content and behavioural change were included in the feedback form
- Each participant received a gadget as a memento of the training session

e-Learning sessions

In the second phase of the project, e-Learning was utilised. E-learning sessions allowed every employee to complete training at their own pace, independent of location. Participation and test measures were captured and made available to the human resources department. No instructors or classrooms were needed.

IT staff training

In addition to general awareness raising, the IT staff were trained on IT security regulations and how to comply with them in their daily work. The objectives were to reduce/mitigate operational risk Training was tailored to the IT staff member's knowledge and experience, job profile and location and department. An e-Lab was provided.

Measurement and supporting material

Several methods were used to measure the performance of the campaign initiative and to gather meaningful feedback:

- Feedback forms - of those who answered, 30% admitted to having a lack of understanding of security issues and 89% said they intended to adapt their behaviour after being trained
- Brochures - communicated and supported by top management, brochures were distributed to all employees. The brochures (available in 5 languages) were sent out two weeks prior to the web questionnaire
- Web questionnaire - these encouraged employees to find the right answers to questions (including referencing supporting material such as the brochures). Follow-up emails were also sent out to further increase awareness. These were well

received. The web questionnaire assessment is now to be repeated every year with different questions

- Security teasers on the Intranet - pull media such as the Intranet had an impact on the number of employees viewing the IT security portal, however the larger impact came from push media such as emails

Lessons learnt

- It's all about humans
- Senior management support is crucial (adopt a top-down strategy)
- Measurement is difficult but very important (create a "before and after" picture)
- Involvement of representatives of the target group in training development is very important (utilise subject matter experts and ensure the training is customized to the target group's needs)
- Address cultural and linguistic differences (important messages must be conveyed in people's mother tongue)
- It's very time consuming to develop and coordinate a group-wide campaign
- To ensure sustainability, on-going activities are needed:
    - Periodic articles in company magazines
    - Keeping the intranet website up-to-date and attractive
    - Monthly "IT Security risk and incident report" to be submitted to top management
    - Yearly measurement of awareness and basic knowledge
- An effective awareness raising campaign can bring about a cultural change
- Don't forget the new people joining the company
- Don't forget the new threads
- Link the content of the campaign to something that could be as well a private issue
- Different modules and level of trainings should be prepared
- Classroom-based training sessions worked better than the e-learning one
- Methods to deliver training should be always reviewed and adjust

Refer to thehumanfactor-isf2004040903_v2.pdf in the *Reference Files* section for more information on the Swiss Re campaign.

Media

Current Situation

Media continues to be used primarily as a communication channel for awareness raising initiatives aimed at other target groups. More Member States are leveraging the media to push campaign messages, however little is being done in the way of educating Media staff with regards to information security.

Country Good Practices

It should be noted that the examples given by the Member States use media as a channel to reach other target groups; no information has been detailed as to raising awareness within the Media target group.

Other Organisation Good Practices

Reuters

The news and media firm has some 16,000 staff in 220 cities in 94 countries around the world – this includes 196 editorial bureaux. Reuters news is seen by over 1 billion people every day.

Reuters is trying to raise awareness in security issues in the same way that SMEs do. The training given to its employees by the firm is targeted to specific audiences based on their skills and their job roles (and hence their needs).

The company has a Group Security Practice - with the firm's main customers being large financial institutions, it is essential that a strong development and security implementation is in place. As a result, a strong security awareness programme is adopted with regards to software development. Architects, Designers, Coders and Quality Assurance personnel are all especially targeted.

The firm uses a variety of delivery channels when trying to get awareness messages across to the relevant target audience. These include:

- Training formats: focused briefings, lunch/breakfast briefings, classroom/workshops and online e-learning
- Marketing and promotion: posters and brochures, security/risk events, games/quizzes/competitions and gifts and giveaways
- Outreach/information dissemination: online references (intranet/extranet), emails and alerts and briefing notes and newsletters
- Feedback: online feedback and staff surveys

It has been noticed that the most effective delivery channels to raise awareness are through classroom or workshop based training. Online e-learning and online references are moderately effective when delivering messages, whereas briefing notes and newsletters tend to be the least effective.

ISP

Current Situation

Collaboration between the public and private sectors and ISPs is increasing within the Member States. More is being done with communicating messages of security to the public, however more can be done with educating ISP staff.

Country Good Practices

France

As part of an initiative to raise awareness for the Young, the French Ministry along with partners from business and society including ISPs, have launched a multi-channel campaign including the distribution of parental control software. For more information, click on the following link to go to the details in the *Good Practices by Country* section for France

Italy

As part of law protecting minors, initiatives focusing on safe surfing-tools and filtering systems has been undertaken. ISP uptake to align with the directive and initiatives has been slow. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Italy

Luxembourg

After an initiative analysing ADSL routers sold in the country, basic content like the secure configuration of routers has been created. The content forms the basis of a close collaboration with ISPs. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Luxembourg

Malta

A joint programme has been launched with an ISP to raise awareness in children. The aim is to introduce children at a young age to the dangers of the Internet. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Malta

Norway

A public-private initiative including ISPs has seen the creation of a website aimed at the general public and SMEs. The website provides information, advice and guidance for secure and safe use of the Internet. The content is grouped into themes and categories. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Norway

Poland

ISPs have been collaborated with on addressing certain IT security issues faced by the general public. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Poland

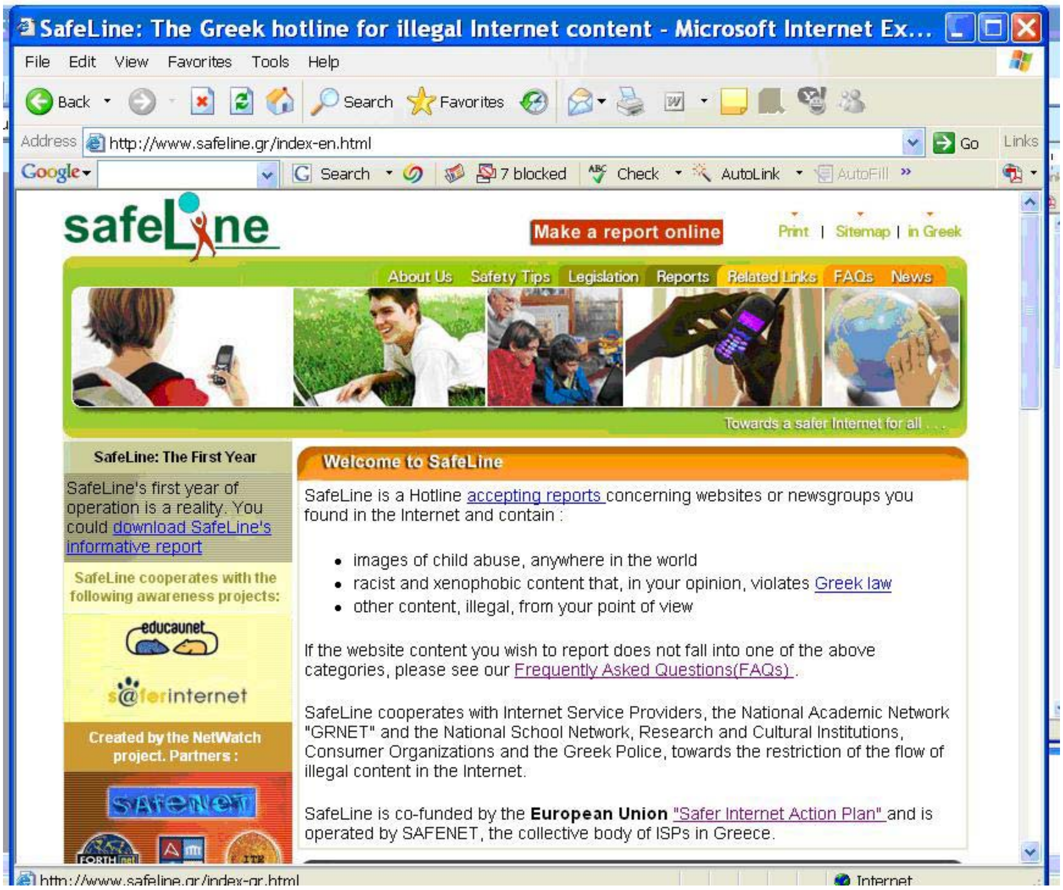
Portugal

Non-government organisations have collaborated with ISPs in trying to address certain IT security issues faced by the general public. Meeting and forums have been used. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Portugal

Other Organisation Good Practices

FORTH

Over the past four years, FORTHnet (one of the largest Greek ISPs), in collaboration with SAFENET, IME, and FORTH, has been running SAFELINE (http://www.safeline.gr), the Greek Hotline in the fight against cyber-crime. SAFELINE has been supported in part by the European Commission, the Greek Government, and the above mentioned partner organisations. SAFELINE has always been active in promoting safer use of the Internet focusing on how to help children and young adults have a safe and fruitful experience on the Internet. To disseminate its activities, SAFELINE organises events, mobilizes the stakeholders in Greece, and collaborates with schools with relevant organisations. Refer below for a screenshot of the portal.


SafeLine: The Greek hotline for illegal Internet content - Microsoft Internet Ex...
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.safeline.gr/index-en.html
Go Links
Google Search 7 blocked Check AutoLink AutoFill
safeLine
Make a report online
Print | Sitemap | in Greek
About Us Safety Tips Legislation Reports Related Links FAQs News
Towards a safer Internet for all . . .
educaunet
s@ferinternet
SAFENET
FORTHnet
ITE
http://www.safeline.gr/index-gr.html
Internet

SafeLine: The First Year

SafeLine's first year of operation is a reality. You could download SafeLine's informative report

SafeLine cooperates with the following awareness projects:

Created by the NetWatch project. Partners :

Welcome to SafeLine

SafeLine is a Hotline accepting reports concerning websites or newsgroups you found in the Internet and contain :

- images of child abuse, anywhere in the world
- racist and xenophobic content that, in your opinion, violates Greek law
- other content, illegal, from your point of view

If the website content you wish to report does not fall into one of the above categories, please see our Frequently Asked Questions(FAQs) .

SafeLine cooperates with Internet Service Providers, the National Academic Network "GRNET" and the National School Network, Research and Cultural Institutions, Consumer Organizations and the Greek Police, towards the restriction of the flow of illegal content in the Internet.

SafeLine is co-funded by the **European Union** "Safer Internet Action Plan" and is operated by SAFENET, the collective body of ISPs in Greece.

Local Government

Current Situation

More and more Member States are starting to specifically target Local Government as part of awareness raising activities. Countries are realising that public sector employees need to be informed of information security issues and protocols, not least as citizens and businesses expect government services to be quick, efficient and issue free. To date, most of the awareness initiatives have been conducted through seminars, training sessions, publications and through the use of online content. Within some Member States, programmes have started that require the collaboration between different agencies or Ministries.

Country Good Practices

Germany

The Federal Government targets people at all levels in an effort to raise awareness. Government employees have also been targeted, for example through the use of manuals. For more information on the general initiatives, click on the following link to go to the details in the *Good Practices by Country* section for Germany

Hungary

There have been several programmes and initiatives aimed at citizens but also civil servants to make efficient use of portals. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Hungary

Ireland

VigiTrust, a private organisation, specialises in awareness raising training for both the public and private sectors. Refer to details in the *Other Organisation Good Practices* section for Local Government.

Italy

An awareness raising initiative in Public Administration aimed at top management, top ICT security managers and employees, is being run. Multiple channels are being used including seminars and web-based e-learning. Employees at the workplace also have the option to voluntarily watch specially created videos. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Italy

Lithuania

As part of Government initiatives, more than 200 people working in state institutions have been trained. The IT security awareness programme is available in either CD or on the web. Seminars and distant learning content for public officials and employees have also been used or is planned to be used. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Lithuania

Luxembourg

A project fully focussed on the security within ministries and administrations has been launched. During the project a risk analysis is being done in the Ministry and an information security policy is being written. The project will deliver awareness raising material specially designed for governmental employees via leaflets, posters, the Intranet and special courses. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Luxembourg

Netherlands

Several initiatives such as ICTU and eGEM aim to promote awareness of security issues with the Local Government target group. For more information, click on the following link to go to the details in the *Good Practices by Country* section for Netherlands

Portugal

Several initiatives have been undertaken or are underway aimed at raising awareness in the Home User, ISP and Local Government target groups. These have mainly been undertaken through training, public events or collaboration. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for Portugal

Sweden

Sweden has conducted or is still conducting various awareness raising initiatives aimed at the Home User, SME and Local Government target groups. Some examples include a project run by the National Post and Telecom Agency which uses interactive websites and publications among other channels, as well as the SurfaLugnt project which has been created with collaboration from the IT industry and relevant authorities. Another initiative, by the City of Stockholm, has seen the creation of a film based on the roles of public sector employees for public sector employees, also covering security guidelines. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for Sweden

United Kingdom

Several awareness raising initiatives have been aimed at the Home User, SME and Local Government target groups. Channels used for delivering awareness messages have included websites, public events, national media (such as TV and radio) and road shows for the public sector. Development programmes such as CSIA also aim to raise national and local cross-Government awareness. For more information, click on the following link to go to the relevant details in the *Good Practices by Country* section for United Kingdom

Other Organisation Good Practices

VigiTrust

VigiTrust do not partner with the Irish government as such in terms of awareness programmes and initiatives. However VigiTrust are engaging with a number of public sector bodies (government departments, local government and semi-rate organisations) to provide security awareness training; this is aimed at raising the overall level of security knowledge throughout of those attending the training. Attendees may choose to attend public workshops where they are taught together with private organisations or choose workshops that can be customized to the requirements of a particular government organisation and be held at their offices.

Target audience description

IT technicians, IT Directors as well as directors or Chief Executives for government departments attend the training with a view to getting more information about the legal, commercial, operational as well as technical aspects of corporate security. In order to raise awareness, VigiTrust look at the business side of security rather than purely concentrating on technical security. Five security pillars are covered: physical security, people security, data security, IT security and disaster recovery/business continuity.

Level of knowledge

This varies and goes form low to high, however most attendee's knowledge before attending the workshop is between medium and low.

Main Issues

The attendees seem to be focused on operational issues such as DR and BC and resolving issues linked to AV outbreaks. Very few are even aware of their responsibilities under the Data Protection Act and other key legislation.

Where customized workshops are being delivered, most attendees have different understanding of the security requirements and countermeasures at their government office. Most of them tend not to have clear policies and those policies that do exist, are not communicated or enforced effectively. To that effect, it would seem that in Ireland the public sector has the same issues and overall level of knowledge in terms of legal requirements as regards to security.

At a technical level, government organisations on average are more advanced than their private firm counterparts for similar size organisations. They will tend to have content filtering for mail and web in place, as well as continually be looking at emerging threats such as USB memory stick usage and desktop threat management.

Value add for attendees – how workshops are increasing security awareness levels

Typically attendees leave with a SWOT analysis on their environment looking at how security can be considered a strength, weakness, threat or opportunity for the organisation. Therefore they leave with a basic benchmark of their knowledge of the security status at their office against best practice. Then they are told how to prioritize action items and how to sort items from what can be done internally by existing staff and what should really be done by external security experts.

The feedback from Irish government customers is that they use the knowledge gained at the workshop as a platform to formulate a plan to further disseminate the concept of security awareness within their department. Very often the organisation will formulate a plan on how to improve security levels based on the findings of the workshops.

Metrics and KPIs

Metrics are not officially in place. The Irish government is trying to raise the overall awareness levels by promoting the makeitsecure day typically help in November (see www.makitsecure.ie). The effectiveness of that campaign can be measured by the attention it gets both from the media and the general public and by the hits on their website. There are a number of security organisations in Ireland which host security information seminars, however most are product focused and commercially orientated. The Global Security Week does not promote any individual product or service. Refer to www.globalsecurityweek.com.

The idea conducting a SWOT analysis of an organisations security is good start to establish a base for that organisation's awareness of key security issues across the five key security pillars. By comparing the results of the first SWOT analysis with the results of a second analysis carried out after an agreed timeframe (e.g. every six months), it is possible to establish the effectiveness of the awareness program by looking at the following items:

- Have all the key threats been addressed?
- Have all the key opportunities to use security as a business enabler, as a company culture enhancement platform and as a productivity enhancement tool been utilized?
- Are the strengths identified in the first SWOT still there and are there more strengths after the second one?
- Have all the weaknesses been eradicated or mitigated?

- Are all employees aware of the changes?
- Are all employees more security aware?

As an example of SWOT analysis results, one could consider the following items (this list is non exhaustive):

Strengths	**Weaknesses**
Best-of-Breed technical solutions are already in place IT staff are aware of the main issues Some policies are already in place Qualified Technical staff holding security accreditation Management are supporting the IT team by way of financial commitment	No general awareness of or commitment to addressing corporate security risks Organisation X not maximising on previous investment on IT system and existing security features. Similar for procedures and policies Day to day focus on security issues as opposed to long term strategy to eradicate issues or address them pro-actively No accountability – No official Security Officer (SO) No policy consistency between the various arms of the group Some policies missing, others need to be updated or rewritten
Opportunities	**Threats**
Additional IT resources are now in place, freeing up time for existing staff to focus more on security topics There is an opportunity to use security to boost productivity, increase system availability and reduce potential liability. This project will also enhance team spirit. Legal aspects of corporate security can be used to get commitment form senior management A new CEO is being appointed – new working practices might be implemented to increase security whose priority level might go up on the agenda	Lack of understanding, commitment and focus from management as regards overall corporate security risks Hackers – no pen testing ever conducted on Rehab's systems DR? – No plan in place Human Behaviour – users not trained at all Reliance on third party security for the Intranet and web-sites, more reliance moving forward when moving to Data Centre

Other ways to measure the effectiveness is to look at the number of security incidents before the awareness program started and after. For instance, how many virus outbreaks have been reported, how many cases of Internet abuse (browsing non-work related and/or offensive web-sites) have been detected, how many employees have received basic awareness training thanks to the program and are these employees more productive than other employees who did not receive the training?

Good Practice Guidelines

Recommendations

General

No.	Guideline	Details
1.	***Plan and implement the initiative appropriately***	Assess requirements and have a clear vision and set of objectives for the campaign. Use plans and phases to help make the tasks and activities more manageable. Also create a Communication Plan. The whole end-to-end awareness raising initiative should be an ongoing and not a static process e.g. re-educating or re-training targets from a previous awareness raising initiative
2.	***Utilise multipliers***	The Media should be used as multipliers for the campaign – they can maximise the reach of an awareness raising campaign by spreading the communications. Other ways to utilise the multiplier effect include training trainers, informing teachers and working with ISPs
3.	***Utilise Public-private partnerships***	Public-private partnership can be a highly effective way to deliver campaigns especially if each organisation can leverage strengths and resources. If a joint programme is developed, it is important to have Codes of Conduct and such elements as Design Guides
4.	***Use multiple channels***	It is important to use multiple channels to deliver the awareness raising message; includes all online and offline medium
5.	***Messages should be meaningful or easily related to***	Content of messages delivered as themes or as usage scenarios can aid in perception and understanding. Also, different target groups may have different levels of understanding or expectations – the message delivered should be tailored and meaningful to the target group's interests, needs and knowledge levels
6.	***Make message noticeable or interactive***	An effective awareness raising campaign to promote security awareness needs to be highly visible and understandable to all. One way is to dispel myths and incorrect assumptions or to show the target the error in their ways. Another way is to make the experience more interactive e.g. using web services on a website to test the strength of the target's password
7.	***Use simple terminology***	Terms and definitions used should be simple to understand to the intended target group
8.	***Use metrics and KPIs***	"What you can measure you can manage" - need to establish metrics to measure the performance of a campaign (also establishing a baseline). Allows for lessons learned to be identified which can help increase the effectiveness of current or future initiatives
9.	***Monitor the awareness raising initiative***	Conducting frequent surveys and reports during or after the campaign can help to fine tune the channels used, message being delivered or overall success of the initiative. Also, it can be important to communicate the success stories, especially to Media

Home User

No.	Guideline	Details
1.	***Use Teachers as a multiplier***	Teachers and the Media should be used as multipliers for any campaign run – they can maximise the reach of an awareness raising initiative by spreading the communications to children
2.	***Stimulate by certifying***	Some sort of Certification programme can interest children to engage more in awareness activities
3.	***Use understandable and identifiable themes***	With the young especially, using simple and common themes and brands can aid in their understanding
4.	***Customise the message***	The needs and interests of the young should be established otherwise the campaign will not appeal to them, resulting in a message landing on deaf ears
5.	***Be creative and draw attention***	There is a need to be inventive and often colourful to raise interest in campaigns for the young. Using channels such as comics or cartoons can help. Also, children can be empowered to help make adults more aware of basic issues
6.	***Create modular or reusable material***	Information or Education Packs have the benefit of being used by the young in schools with their teachers or at home with their parents. Learning kits can be effective as it can get the whole family involved
7.	***Use specific channels***	Health care stations and social security institutions are effective ways to communicate with Silver Surfers
8.	***Get back to basics with the message***	The messages conveyed to raise awareness for Silver Surfers should go back to basics when possible as the generations grew up without ICTs

SME

No.	Guideline	Details
1.	***Use efficient channels***	With the abundance of online information and with time often a premium asset, using channels such as brochures, leaflets and fact sheets are very effective to get attention and hence raise awareness
2.	***Use specific channels***	Using trade organisations, workshops, seminars and partner initiatives are all effective ways to target Directors or business owners. Specialist channels such as online computer sites or trade journals can be effective when targeting IT personnel due to the relevance to their day-to-day work. The use of agencies such as the local chambers of commerce, SME-union networks, trade associations or business journals are all effective channels for Business Managers
3.	***Get backing from other organisations***	Working with other government departments or agencies can give more credit to any campaign aimed at SMEs
4.	***Customise the message***	Where possible, the campaign message and channels used should be customised to the category level of the SME and be adapted to roles and responsibilities
5.	***Raising awareness is not a one time effort***	As there is continual change, an ongoing programme of security education or training is hugely important to raise awareness in employees on the risks to information security

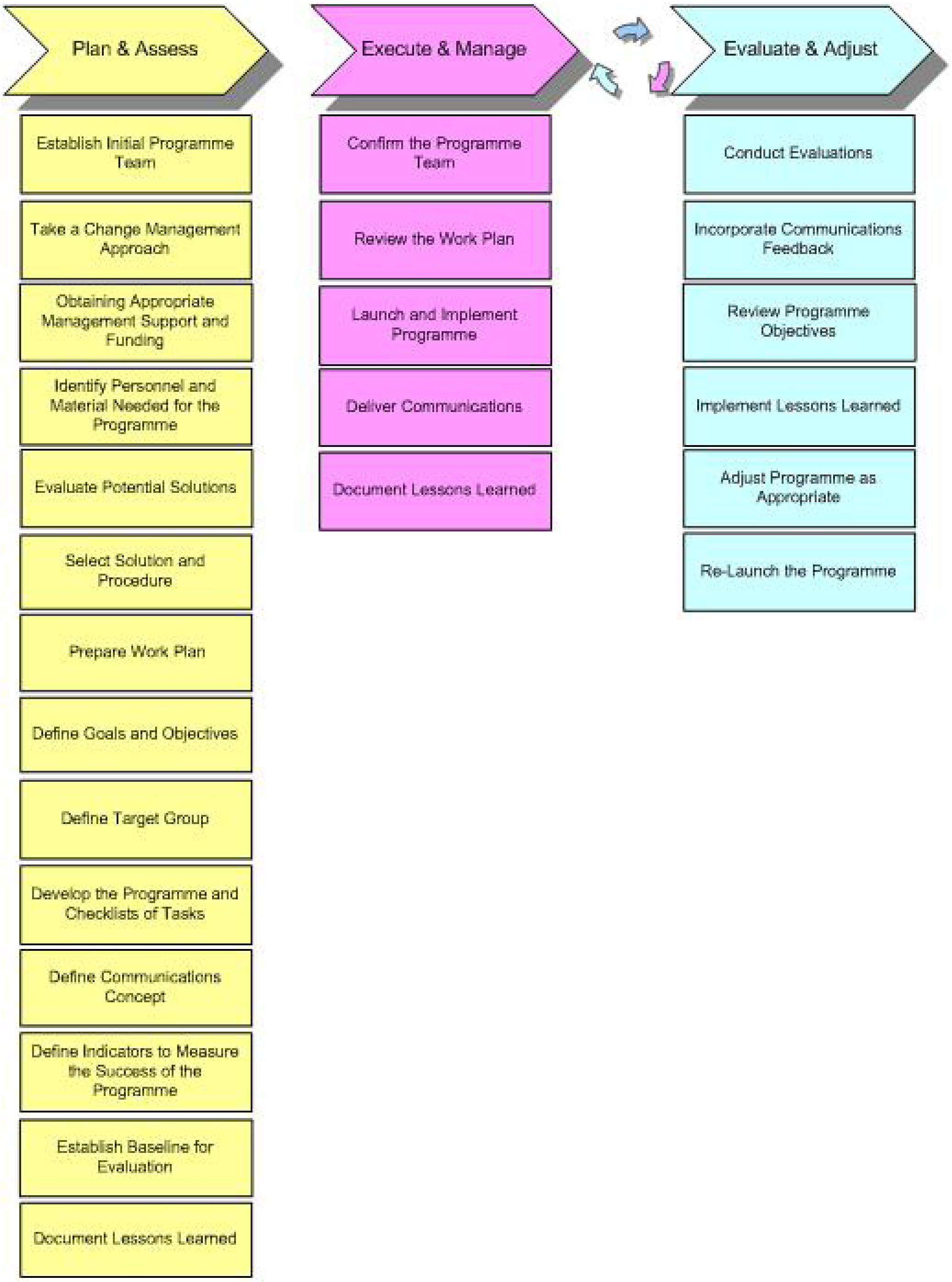
6.	***Use channels within the workplace***	Effective employee awareness can be achieved by the successful implementation of information security policies. These include the user of staff handbooks and manuals, contracts and letters of employment, induction exercises and training courses or ongoing on-the-job training

Media

No.	***Guideline***	***Details***
1.	***Understand the importance of media to the public***	It may be useful to send a message that the Media has a social responsibility for the reporting of accurate information and that the information disseminated by them should be of high quality. By it's very nature, information security risks have the potential for ruining the confidentiality, integrity and availability of information, meaning that's it certainly a key topic of interest for them
2.	***Create networks and partnerships***	Building trust and a relationship with the Media can help in getting coverage for awareness raising activities
3.	***Customise the message***	Dedicated Press briefings or information packs for the Media can help to focus and ease their efforts on reporting information security topics
4.	***Use specific channels***	Apart from press kits and other collateral (such as articles and fact sheets), building an online presence or repository of information dedicated to the Media target group could make it easier for them to first raise awareness within their own community, and then to raise awareness in the public. Training sessions and workshops for journalists are other means in which to relay awareness related messages
5.	***Keep them interested***	Offering regular updates on topical subjects or directly contacting the Press Association can be an effective method of keeping the Media aware and involved

Checklists

When designing, implementing and executing any type of awareness raising initiative, the tasks and activities required can be grouped into three main phases. As detailed in the ENISA "A User's Guide: How to Raise Information Security Awareness" document, the phases and components can be illustrated as follows:



Plan & Assess
Establish Initial Programme Team
Take a Change Management Approach
Obtaining Appropriate Management Support and Funding
Identify Personnel and Material Needed for the Programme
Evaluate Potential Solutions
Select Solution and Procedure
Prepare Work Plan
Define Goals and Objectives
Define Target Group
Develop the Programme and Checklists of Tasks
Define Communications Concept
Define Indicators to Measure the Success of the Programme
Establish Baseline for Evaluation
Document Lessons Learned
Execute & Manage
Confirm the Programme Team
Review the Work Plan
Launch and Implement Programme
Deliver Communications
Document Lessons Learned
Evaluate & Adjust
Conduct Evaluations
Incorporate Communications Feedback
Review Programme Objectives
Implement Lessons Learned
Adjust Programme as Appropriate
Re-Launch the Programme

Breaking each phase down into tasks and activities, checklist items can be constructed. Member States should use these as guidance for the main steps to undertake when running any kind of information security awareness raising programme:

I. Plan and Assess

No.	Checklist item
1.	☑ **Establish initial programme team:** setup a programme team primarily for the first phase but with a view to transitioning them into subsequent phases (for continuity). Ensure roles and responsibilities clearly defined
2.	☑ **Take a change management approach:** adopt and implement a change management methodology to ensure that the campaign objectives are reached and ultimately the target group's awareness and behaviour is changed
3.	☑ **Obtain appropriate management support and funding:** get stakeholder/senior management buy-in and support. Look for public-private partnerships where possible. Cost Benefit Analysis can help when trying to identify funding needs and identifying programme benefits can help with getting buy-in and funding
4.	☑ **Identify personnel and material needed for programme:** ensure programme team and resources sufficiently skilled and experienced, covering areas in IT, HR, communications and training and development. Utilise knowledge from Member States and other information repositories such as the Internet for identifying potential solutions
5.	☑ **Evaluate potential solutions:** when evaluating potential solutions, consider public-private partnerships or whether the awareness programme can be planned and executed in-house or needs to be outsourced
6.	☑ **Select solution and procure:** after careful evaluation, select the best solutions and organisations to implement the awareness programme
7.	☑ **Prepare work plan:** start building a work plan and include the main activities for which the required resources, timescales and key milestones need to be identified
8.	☑ **Define goals and objectives:** in order to effectively plan, organise and evaluate an awareness programme, the programme goals and objectives need to be identified
9.	☑ **Define target groups:** it is critical to identify and define the specific group that is targeted by the awareness initiative. Each target group has unique interests and needs, as well as operating in different environments
10.	☑ **Define the programme and checklist of tasks:** efforts should be focused on designing the programme and on further developing and implementing the plan. Key messages should also be identified and developed
11.	☑ **Develop communications concept:** an effective and efficiently implemented communication plan is critical to the success of an awareness programme. A strategy should be constructed identifying bodies/organisations that can be used as multipliers as well as which ones can be used as partners. The content of messages needs to be further developed and tested, and appropriate communication channels identified
12.	☑ **Define indicators to measure the success of the programme:** in order to measure the performance of an awareness programme, it is imperative to clearly identify and construct metrics and key performance indicators
13.	☑ **Establish baseline for evaluation:** apart from identifying metrics and key performance indicators, the current situation with regards to the target group needs to be understood. This way, the effectiveness of an awareness programme can be measured based on the change in landscape
14.	☑ **Document lessons learned:** get the programme management and teams involved in capturing lessons learned from activities completed in the first phase

II. Execute and Manage

No.	Checklist item
1.	☑ **Confirm programme team:** before launching the programme, confirm the team that will be responsible for both execution and obtaining results. Each member of the awareness raising team should have a specific role and set of responsibilities when implementing and managing the initiative
2.	☑ **Review the work plan:** the work plan needs to be updated and programme milestones finalised. This has to be completed before launch, as the awareness raising team need to be aware of, and comply with, the goals and objectives as well as budget requirements and project constraints
3.	☑ **Launch and implement programme:** at this stage of the programme, all the protocols and arrangements should be in place and ready to go. The awareness raising team and all partners should carry out any execution tasks or activities defined and assigned to them in the work plan
4.	☑ **Deliver communications:** the communication plan should be implemented and associated messages delivered to the applicable target groups via the designed channels. As part of the metrics and key performance indicators, as well as capturing lessons learned, it is important to try to collect feedback on the communications
5.	☑ **Document lessons learned:** repeat similar procedures as those used to capture lessons learned at the end of the first phase. Compare the historical evolution of the programme from a learning perspective

III. Evaluate and Adjust

No.	Checklist item
1.	☑ **Conduct evaluations:** in order to understand the performance of the programme and to try to quantitatively or qualitatively measure the effectiveness in raising information security awareness and hence reducing security incidents, data should be collected. Follow-up questionnaires and omnibus surveys are one way to conduct the evaluations
2.	☑ **Incorporate communications feedback:** the feedback captured when delivering the programme's communications should be reviewed with a view of improving future plans. The information should be combined with the results derived from the evaluation metrics
3.	☑ **Review programme objectives:** the success of an awareness programme can largely be decided by the outcomes in relation to the original objectives. If the programme is ongoing, then the original objectives may need to be revisited in light of the performance
4.	☑ **Implement lessons learned:** the lessons learned from the previous phases combined with the feedback based on the communication plan, should be leveraged to make the ongoing or future programmes more effective. It is important to learn from both the successful and less successful activities
5.	☑ **Adjust programme as appropriate:** if the programme is ongoing or to be re-launched, the experiences gained to date should provide knowledge and understanding to adjust the programme to make it more successful. Adjustments should be made while maintaining the focus on the programme goals and objectives
6.	☑ **Re-launch the programme:** when re-launching the adjusted programme, tasks as identified in Phase II should be repeated. More effort should be funnelled towards those activities that maximise the effectiveness of the awareness raising programme

For more information on any of the phases and subsequent checklist items, refer to the ENISA User Guide.

Metrics/KPIs

Definitions

Metrics - A system of parameters or methods of quantitative assessment of a process that is to be measured, along with the processes to carry out such measurement.

Metrics can develop and change based on growing insight over time. Some metrics are stand-alone whereas others are interdependent. They can be further broken down or detailed through key performance indicators.

Key performance indicators (KPIs) - Quantifiable metrics used to evaluate objectives to reflect the performance of an organisation. The KPIs differ depending on the nature of the organisation. Different layers and dimensions should be taken into consideration.

KPIs can constitute both quantitative and qualitative measures, however the most useful and common types are quantitative based. These include amongst others focus on metrics such as number of citizens targeted, number of security incidents in the last year compared to the previous year and number of hits to the website.

To help define performance targets and measurements (including use of metrics and KPIs), several industry standard performance management models such as Balanced Scorecard or Six Sigma can be used.

Evaluating effectiveness

Many public and private organisations that have launched awareness raising initiatives within the Member States have not put in place metrics or defined KPIs that can be used to quantify the value of the awareness programme. Evaluation of the executed campaigns is essential in order to gather lessons learnt and to apply them to future initiatives; this way, not only can the future programmes be even more effective, but more fundamentally, organisations will be able to track whether the awareness programmes are improving information security within businesses and citizens alike.

Dealing with target groups

It is important to understand that the same evaluation metrics cannot be universally applied to all target groups since interests and needs, as well as the user’s situation differ greatly between the different groups.

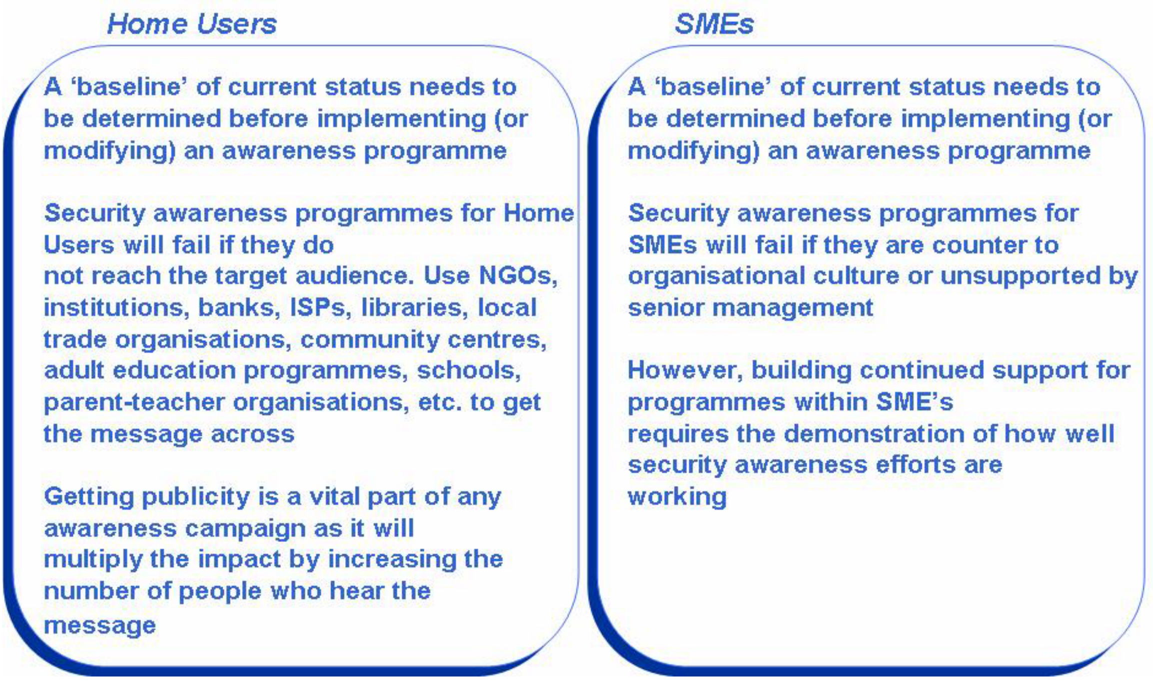
When trying to identify metrics for evaluating campaigns aimed at the Home User and SME target groups (the most widely targeted groups in information security awareness initiatives), a couple of key observations should be noted:

- Awareness programmes aimed at SMEs should focus on the need to develop and implement an information security policy as well as suggesting means of compliance to the policy within the organisation. This also applies for organisations in the public sector
- Public authorities are not necessarily in a position to develop information security policies for Home Users. Focus should therefore be on developing “recommended guidelines” or “best practices” in information security and to promote them to the public

Tools used primarily in business such as the PESTEL (Political, Environmental, Social, Technological, Ecological and Legal) analysis can be used for better understanding the various external influences on the target groups.

Identifying critical success factors

In coordination with trying to identify target group specific metrics and KPIs, it is essential to identify the critical success factors for the relevant target group. These should be the key criteria that will maximise the chances for a positive behavioural impact on the target group by the executed awareness raising programme. For example:



Home Users

A ‘baseline’ of current status needs to be determined before implementing (or modifying) an awareness programme

Security awareness programmes for Home Users will fail if they do not reach the target audience. Use NGOs, institutions, banks, ISPs, libraries, local trade organisations, community centres, adult education programmes, schools, parent-teacher organisations, etc. to get the message across

Getting publicity is a vital part of any awareness campaign as it will multiply the impact by increasing the number of people who hear the message

SMEs

A ‘baseline’ of current status needs to be determined before implementing (or modifying) an awareness programme

Security awareness programmes for SMEs will fail if they are counter to organisational culture or unsupported by senior management

However, building continued support for programmes within SME’s requires the demonstration of how well security awareness efforts are working

Establishing a baseline for evaluation

To be able to use metrics and KPIs to measure the success or impact of an awareness raising programme, a baseline of the current status of the environment needs to be established. By determining the target group situation beforehand, it is possible to track the benefits brought about by the awareness programme.

Questionnaires and omnibus surveys are one way in which to evaluate the effectiveness of programmes. If this data gathering method is used for example, it is important to note that similar questionnaires and surveys should be re-used at future stages of the initiative once the campaign has been executed. This allows for a post-initiative evaluation to be compared against the baseline.

Ensuring accurate measurement

When trying to use metrics and KPIs to measure the performance of campaign, a few key steps should be undertaken to ensure the accurate measurement of the value of the awareness programme:

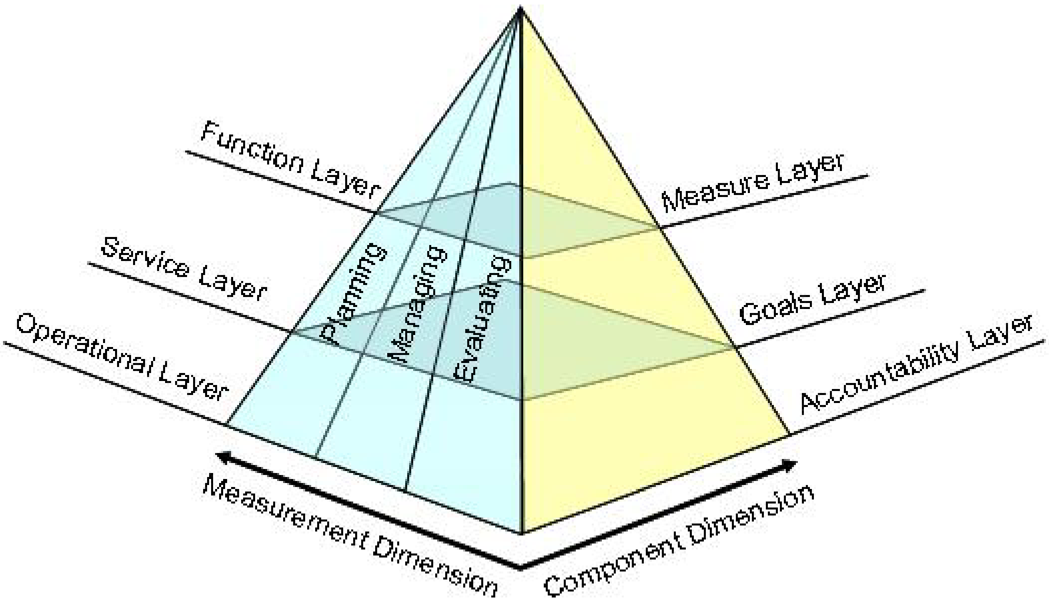
1. Define processes, tasks and activities necessary to run an awareness campaign
2. Identify metrics and KPIs for measuring security awareness
3. Map KPIs to the appropriate processes and activities

1. Define processes, tasks and activities

In addition to the items as detailed in the *Checklists* section, processes and campaign specific tasks and activities should be clearly identified at the start of any awareness raising initiative. Each process usually needs its own performance indicators and measures. Some of the processes and steps therefore will be mapped against metrics/KPIs to allow the specific progress and results to be monitored and reported on.

2. Identify metrics & KPIs

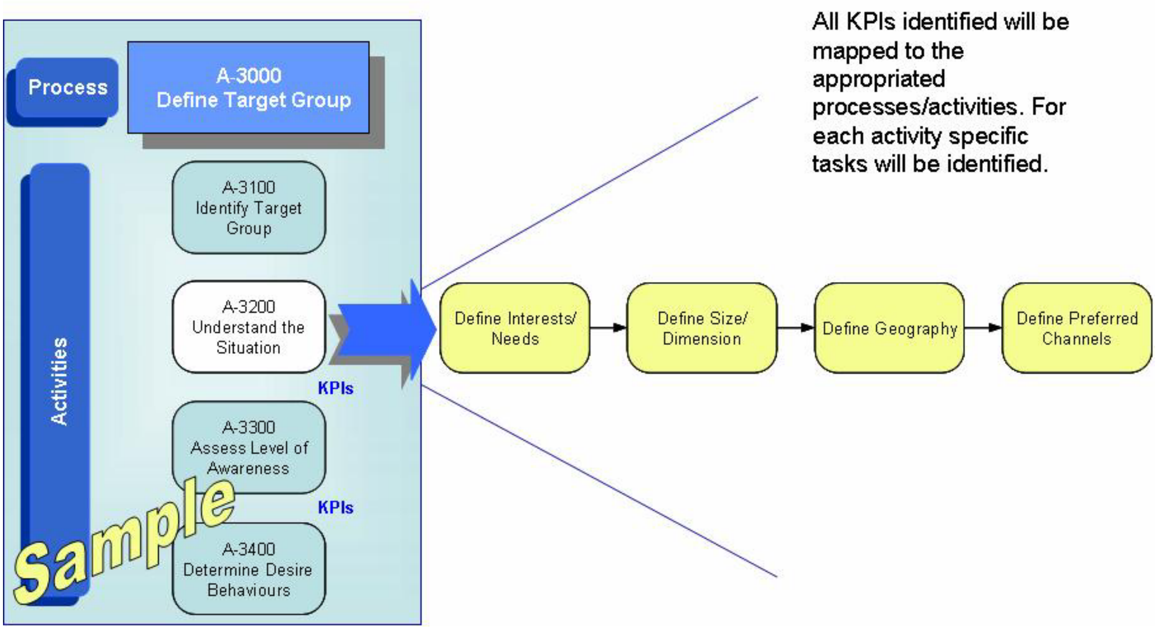
When constructing metrics and KPIs, different layers and dimensions should be taken into consideration:



Refer to the sample_kpis.pdf document for example KPIs that can be used when trying to measure the effectiveness of an awareness raising initiative. The document lists example KPIs that have been compiled from multiple sources.

3. Map KPIs to processes

After the processes, tasks/activities and metrics/KPIs have been identified, it is possible to map the various entities together. This process will ensure that every relevant step is appropriately tracked and measured:


Process
A-3000
Define Target Group
Activities
A-3100
Identify Target Group
A-3200
Understand the Situation
KPIs
A-3300
Assess Level of Awareness
KPIs
A-3400
Determine Desire Behaviours
Sample
Define Interests/ Needs
Define Size/ Dimension
Define Geography
Define Preferred Channels
All KPIs identified will be mapped to the appropriated processes/activities. For each activity specific tasks will be identified.

Measuring effectiveness

Security awareness can be measured by using and adapting the metrics as proposed by Gartner. Four categories can be used when measuring the success of any security awareness programme:

- *Process Improvement:* This category deals with the development, dissemination and deployment of recommended security guidelines as well as awareness training. Example evaluation metrics include:
  - Home User - what percentage of individuals surveyed know that recommended security guidelines exist? How many have seen or read them?
  - SME - what percentage of the employees know that a security policy exists? How many have read it?
- *Attack Resistance:* This category is concerned with recognition of a security event and resistance to an attack. Example evaluation metrics include:
  - Home User - what percentage of users failed testing to reveal their password?

    - SME - what percentage of IT administrators or helpdesk personnel failed to prevent an improper password change attempt?
- *Efficiency and Effectiveness:* This category is focused on efficiency and effectiveness with regards to security incidents. An example evaluation metric includes:
    - Home User/SME - what percentage of security incidents experienced by individuals had human behaviour as a majority factor in the root cause?
- *Internal Protections:* This category is concerned with how well an individual is protected against potential threats. An example evaluation metric includes:
    - Home User/SME - what percentage of an individual's system has pirated software installed?

Gathering data

It is recommended that a combination of quantitative and qualitative information be captured when collecting data by which to measure the performance of awareness raising initiatives. The data should be continually captured (as measuring performance and monitoring the effectiveness of an initiative should be done during and after execution), and should ideally be caught through automated processes.

Methods to capture data include among others: questionnaires, website statistics, general observations, statistics from data centres, focus groups, data from call centres/hotlines, number of reports to IT support, press clippings, newsletters, press releases, number signed up to online services and number of people trained.

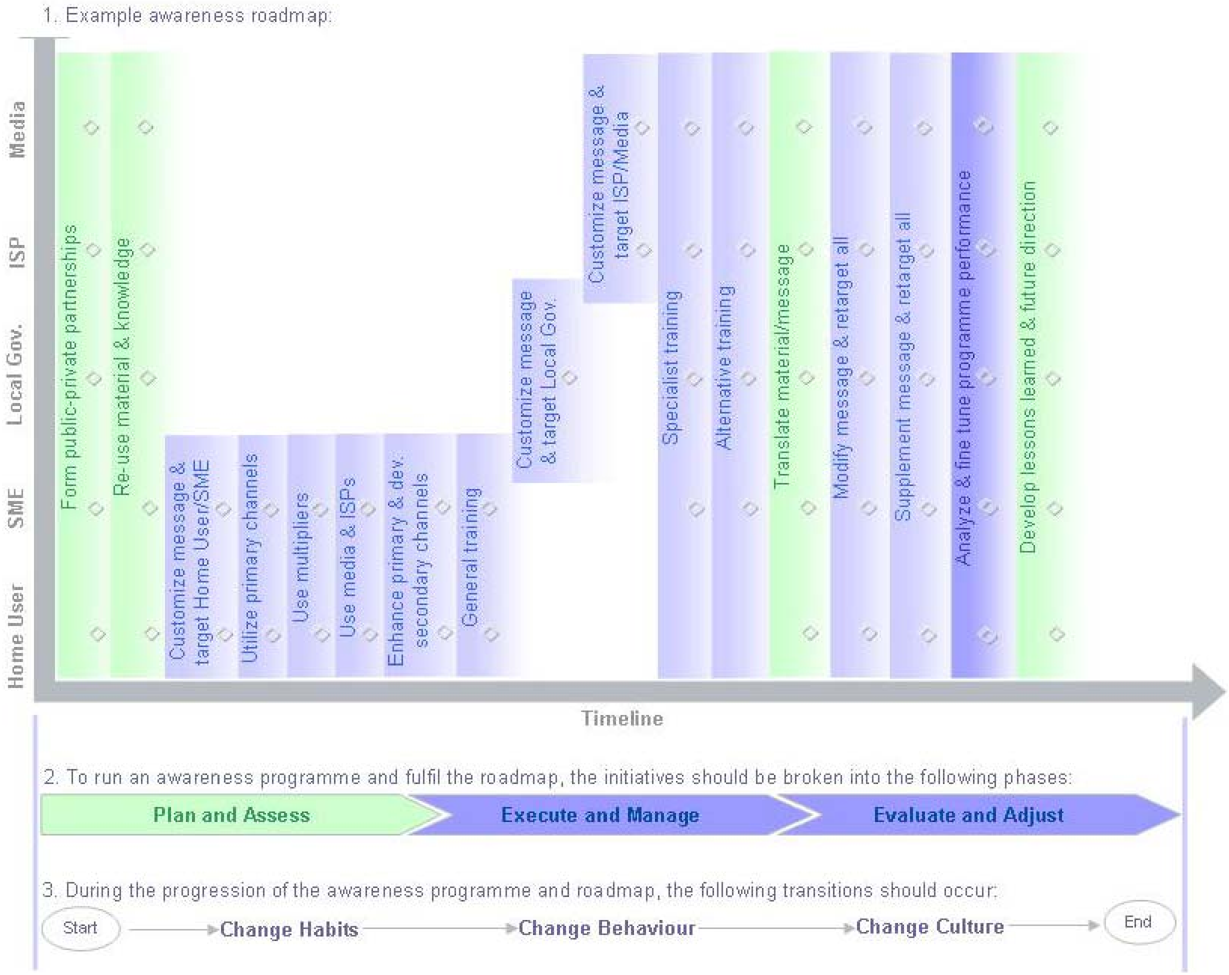
Refer to the *Define Indicators to Measure the Success of the Programme* section in the ENISA User's Guide (enisa_a_users_guide_how_to_raise_is_awareness.pdf) for more detail on using metrics and KPIs as part of an awareness raising initiative.

Roadmap

The following diagram illustrates how a Member State could outline and implement an awareness roadmap to help contribute to a culture of information security awareness. The diagram should only be used as an example (as the strategy, tasks and activities can vary depending on the country's objectives and its current situation).

When viewing the diagram, refer to the colour key below which aids to group together roadmap items:

Colour Key:	
🟩	Roadmap item is typically done one time and hence does not need to be continually undertaken. In some instances, the set of tasks and activities may be repeated but only in a minor capacity
🟪	Roadmap item is typically done in sequence and is ongoing from that point onwards. The set of tasks and activities are therefore continually performed after initiation
🟦	Roadmap item is typically done at the start, during and at the end of the awareness programme. The set of tasks and activities are therefore continually performed throughout the initiative lifecycle


1. Example awareness roadmap:
Media
ISP
Local Gov.
SME
Home User
Form public-private partnerships
Re-use material & knowledge
Customize message & target Home User/SME
Utilize primary channels
Use multipliers
Use media & ISPs
Enhance primary & dev. secondary channels
General training
Customize message & target Local Gov.
Customize message & target ISP/Media
Specialist training
Alternative training
Translate material/message
Modify message & retarget all
Supplement message & retarget all
Analyze & fine tune programme performance
Develop lessons learned & future direction
Timeline
2. To run an awareness programme and fulfil the roadmap, the initiatives should be broken into the following phases:
Plan and Assess
Execute and Manage
Evaluate and Adjust
3. During the progression of the awareness programme and roadmap, the following transitions should occur:
Start
Change Habits
Change Behaviour
Change Culture
End

Roadmap Item Key:
Form public-private partnerships – e.g. ranging from IT companies through to community organisations
Re-use material & knowledge – e.g. use programme material and expertise from other Member States if applicable
Customize message & target Home User/SME – e.g. construct and deliver key target group specific messages
Utilize primary channels – e.g. develop and launch websites
Use multipliers – e.g. leverage positions such as teachers that can reach a wider audience
Use media & ISPs – e.g. collaborate with and use media and ISP as communication channels
Enhance primary & development secondary channels – e.g. increase functionality of websites (making more interactive) or deploy other channels such as telephone hotlines
General training – e.g. public events and awareness training sessions for the general public
Customize message & target Local Government – e.g. construct and deliver key target group specific messages
Customize message & target ISP/Media – e.g. construct and deliver key target group specific messages
Specialist training – e.g. classroom based or train-the-trainer sessions covering role specific functions
Alternative training – e.g. e-learning training programs
Translate material/message – e.g. make campaign messages multi-lingual
Modify message & retarget all – e.g. add to key messages covering topics such as WiFi or mobile phone security
Supplement message & retarget all – e.g. add further detailed or organisation specific messages such as the use of pull-print technology to make printing and scanning devices more secure
Analyze & fine tune programme performance – e.g. benchmark against baselines and use metrics and key performance indicators
Develop lessons learned & future direction – e.g. compile recommendations and also knowledge transfer wit teams and Member States

Other Reading

Recommended Reading

- The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, Working Party on Information Security and Privacy, Dec 2005 (document)
- OECD Annual Report, 45th Anniversary, 2005 (document)
- Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2003 (document)
- OECD Culture of Security Web Site, http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
- A Users' Guide: How to Raise Information Security Awareness (document)
- Measuring effectiveness of awareness programmes (presentation)

Electronic Files

The following electronic files have been referenced within the Information Package 2006:

File	Language
2005_33_sakerhetsinfo_internetanv.pdf	Swedish/Eng.
accord_afa_famille_avec_logo.pdf	French
banniere_cegetel3.gif	French
charte_d'engagements_des_op_contenu_multimédia-signée.pdf	French
dti_info_security_2006.pdf	English
e-crime_wales_action_plan_final2.pdf	English
enisa_a_users_guide_how_to_raise_is_awareness.pdf	English
enisa_info_security_awareness_programmes_eu.pdf	English
enisa_questionnaire_2006_v.5.0_final.pdf	English
neufkit2.jpg	French
oecd_annual_report_2005.pdf	English
oecd_implementation_plan.pdf	English
ppp_for_a_safer_internet.pdf	English
report_on_the_promotion_of_a_culture_of_security.pdf	English
safenethome_annualreport2005.pdf	English
sample_kpis.pdf	English
sweden_survey.pdf	English
the_threats_english.pdf	English
thehumanfactor-isf2004040903_v2.pdf	English
us_national_cyber_security_awareness_month_2005_summary_2.pdf	English