enisa
European Network
and Information
Security Agency

# CD Information Package:

## Raising Awareness in Information Security - Insight and Guidance for Member States

Full Text for CD Application - Not for Unauthorised Distribution

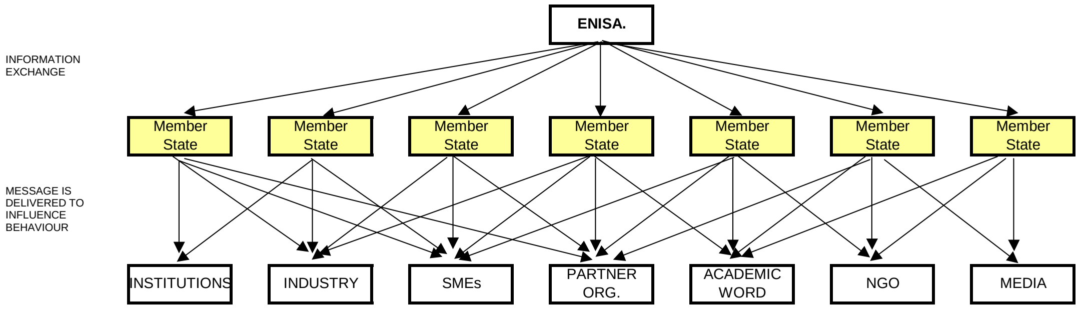
December 2005

# Table of Contents

# Summary

The current environment in which we live and operate in demands a “culture of security” so as to protect Information Communication Technology (ICT) users from information security breaches. Even with the faster propagation and sophistication of new attack techniques, the biggest risk to protecting digital information remains human error. Security policies and procedures in the workplace or additional security controls at home in itself do not minimise the ability of intruders to compromise information. As it is therefore the human component that is critical in any effective and robust security framework, any initiative to increase the awareness of ICT users so as to positively influence their secure behaviour, should have a significant effect on mitigating information security related incidents.

ENISA and many Member States have already realised the importance of their role in creating a culture of greater self-awareness of information security. ENISA serves as a centre of expertise that facilitates information exchange and cooperation. Reviews of already implemented good practices have revealed that Member States can positively influence the public’s behaviour towards information security. These good practices also reveal that communications utilising the messages that appeal to the right Target Group are of prime importance to the effectiveness of any awareness-raising initiative.



For an effective campaign to positively influence the behaviour of the Target Group, the audience has to first be properly evaluated. The interests, needs and knowledge of the Target Group should be identified so as to allow the message that is delivered as part of any initiative to be perceived as one of personal value or interest. The communication channels need to be investigated so as to optimise the delivery of the campaign message. By identifying the preferred communication channels for Target Groups, the campaign has more chance of success. Establishing the most effective channels to use can be done through utilising focus groups or surveys for example. Awareness in general relies on reaching broad audiences with attractive and/or appropriate packaging techniques. It is worthwhile therefore to investigate good practices for raising awareness in areas outside of information security,

for example by learning from drink driving or anti-smoking campaigns.  Also, more measurements of success need to be captured so as to establish the effectiveness of any awareness-raising initiative.  Establishing lessons learnt and capturing quantitative and qualitative data can be used to help improve future campaigns.  Finally, greater and more clearly defined co-ordination or partnerships, for example through public-private or cross-Member State initiatives, can lead to maximising the potential reach of any campaign.

# Introduction

In the digital age where we now find ourselves living and working, individual citizens and businesses alike have found the use of ICT’s to be invaluable in day-to-day tasks.

However, with vulnerabilities in these new and existing as well as with the convergence of these technologies, the growing use of “always on” connections and the continuous and exponential user uptake within Member States, more and more citizens and businesses are now at risk of information security breaches. These security breaches may be IT related, for example through the execution of computer viruses, or may be socially motivated, for example through physical theft of equipment. In an age ever more reliant on digital information, there are an increasing number of dangers, with a considerable number of citizens still being unaware of the exposure to the risks to their security.

With the advancements and proliferation of these dangers, information security solutions used today will be obsolete when looking to tomorrow. The security landscape is continually changing – but if as most analysts report it is the human component of any information security framework that is the weakest link, then only a significant change in user perception or organizational culture can really reduce the number of information security breaches.

When home users in many of the Member States are still not aware of, for example, the fact that their personal computers can be controlled without their knowledge by hackers with the intent of electronic identity fraud or as part of a network to launch a Denial of Service attack, then there is clearly a significant shortcoming in information security awareness.

ENISA is working in advising and assisting the Member States to develop a better understanding of awareness-raising and its effects and to help propagate the measures and their best use.

## *Scope*

The purpose of this document is for ENISA to provide details on awareness-raising initiatives related to information security that have been conducted in Member State countries. Through examples of the good practices and high-level analysis, the Agency has also constructed a basic communication framework to help form the basis of an effective and targeted awareness campaign.

The country case studies used as part of this document should be seen as examples of good practices for awareness-raising campaigns, based on the implementation and success in

Member State countries. The examples should not necessarily be regarded as "Best Practices" as the performance data captured on executed campaigns does not allow for objective comparisons.

This document should also not be seen as 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*

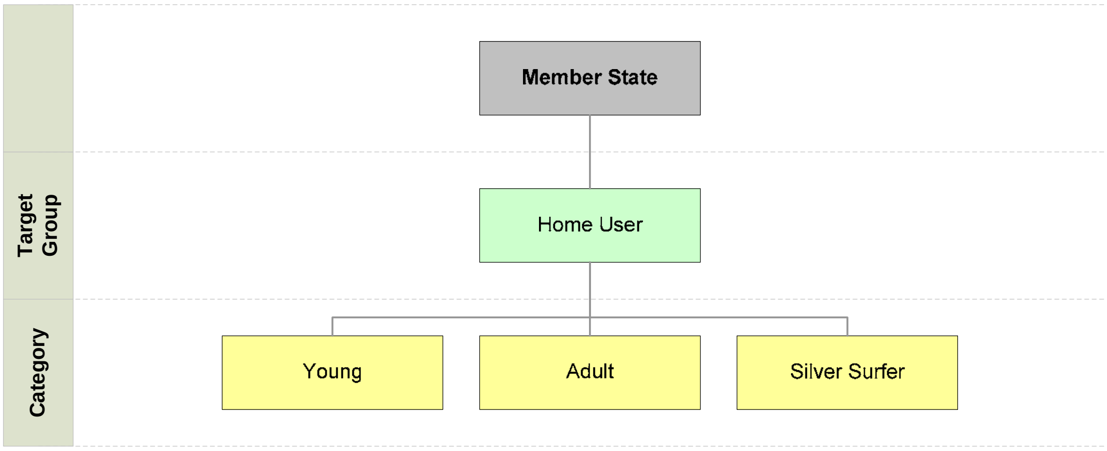
The aims of this document are for ENISA to:

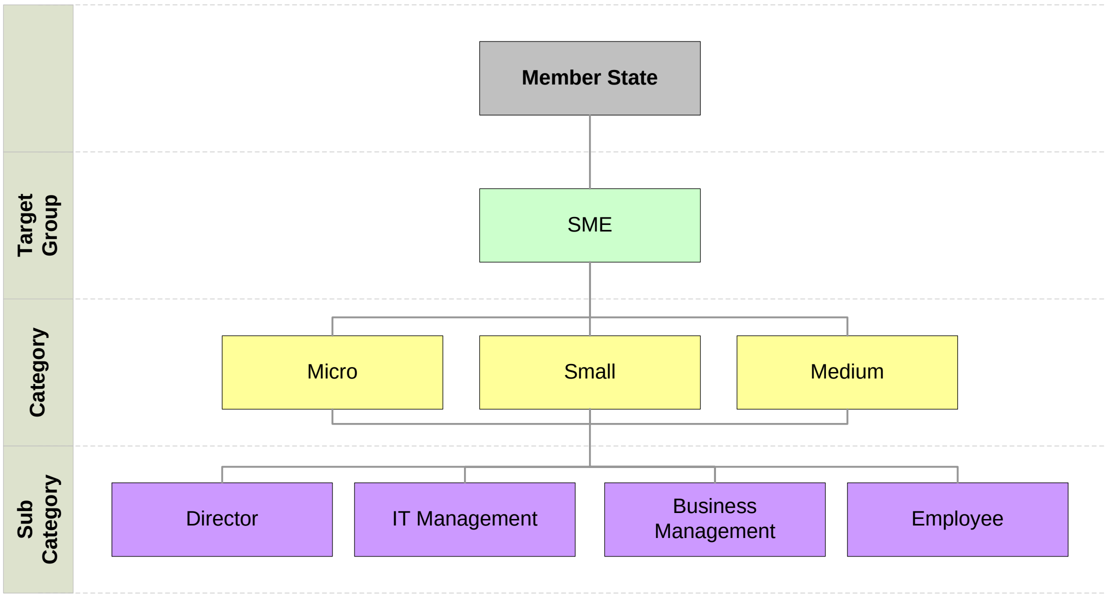
- Offer an insight into the types of problems currently being faced by countries with regards to information security
- Illustrate examples of campaigns and other awareness-raising initiatives that have been run or are planned to run in Member State countries
- Provide examples of some of high level non technical messages that should be conveyed in a typical campaign
- Offer a communication framework based on country examples
- Contribute to the development of an information security culture in Member States by encouraging users to act responsibly and thus operate more securely

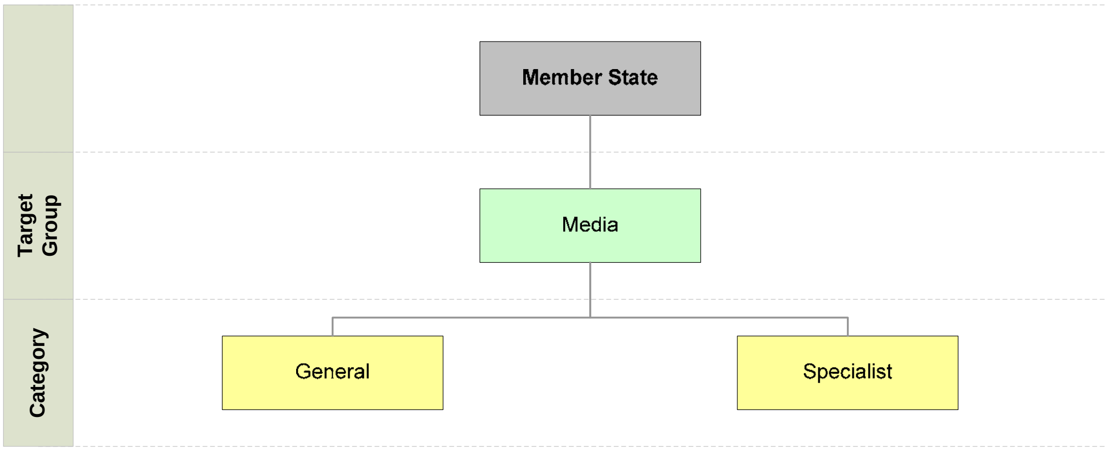
## *Target Audience*

This document is aimed specifically at EU Member States for use when conducting awareness-raising campaigns.

The focus is on three Target Groups: Home Users, Small and Medium Enterprises (SME's) and Media. Descriptions on each group can be found in the Profile of Groups section. Graphically, these three Target Groups can be illustrated as follows:


Target Group
Category
Member State
Home User
Young
Adult
Silver Surfer


Target Group
Category
Sub Category
Member State
SME
Micro
Small
Medium
Director
IT Management
Business Management
Employee


Target Group
Category
Member State
Media
General
Specialist

As the most essential ingredient of any successful campaign is to ensure that the channel used and message conveyed specifically meet the needs, interests and knowledge of the targeted profile of citizens, this document will look to focus on these three selected groups.

It is worth noting that there are numerous ways to establish the particular profile of citizens to target as part of any awareness-raising initiative. For example, the campaign can target users based on age group, social demographics, geographic location or job profiles. The campaign could also be targeted to collective group entities such as Institutions, Non Government Organisations (NGOs), Universities or in the case of this document, to Home Users, SME's and the Media.

## *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.

The United Kingdom Department of Trade and Industry (DTI) in accordance with International Standards such as ISO 17799, describe the three pillars or classifications of Information Security as:

- ***Confidentiality****:* ensuring the information is accessible only to those authorised to have access
- ***Integrity:*** protecting the accuracy and completeness of information
- ***Availability****:* ensuring that access to information is available when and where required and is not denied to any authorised user.

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 Information Security Breaches Survey 2004 commissioned by the 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 as 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
- 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.[1]

It is therefore critical that the first line of defence, people, are suitably 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 by advising and assisting Member States and the EU bodies to ensure a high and effective level of security. ENISA serves as a centre of expertise that facilitates information exchange and cooperation.

**Contact Details:**
Isabella Santa, Florent Sagaspe
e-mail: awareness@enisa.eu.int

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

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

**Legal Notice:**

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

Notice must be taken that information contained in this document has been compiled by ENISA staff on the basis of information that is publicly available or has been supplied to ENISA by appropriate organisations within the EU Member States. This document 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 contained in this publication. ENISA is not responsible for the content or the external web sites referred to in this publication.

No part of this document may be reproduced in any media except as authorised by written permission and provided that the source is acknowledged.

## *Glossary*

The following table details the technical terms with associated definitions used within this document:

| *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 |
| ***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 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*** | |

| ***Term*** | **Definition** |
|---|---|
| *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 |
| | |

# Good Practices

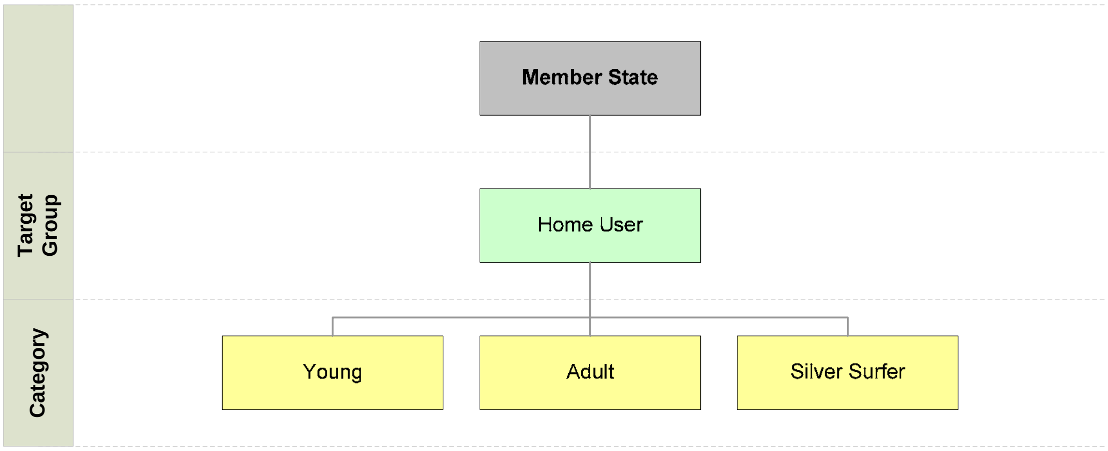
## *Profile of Groups*

Before detailing the profiles of the three Target Groups focused on in this document, 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 or Media |
| *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 ICT's 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 three Target Groups:

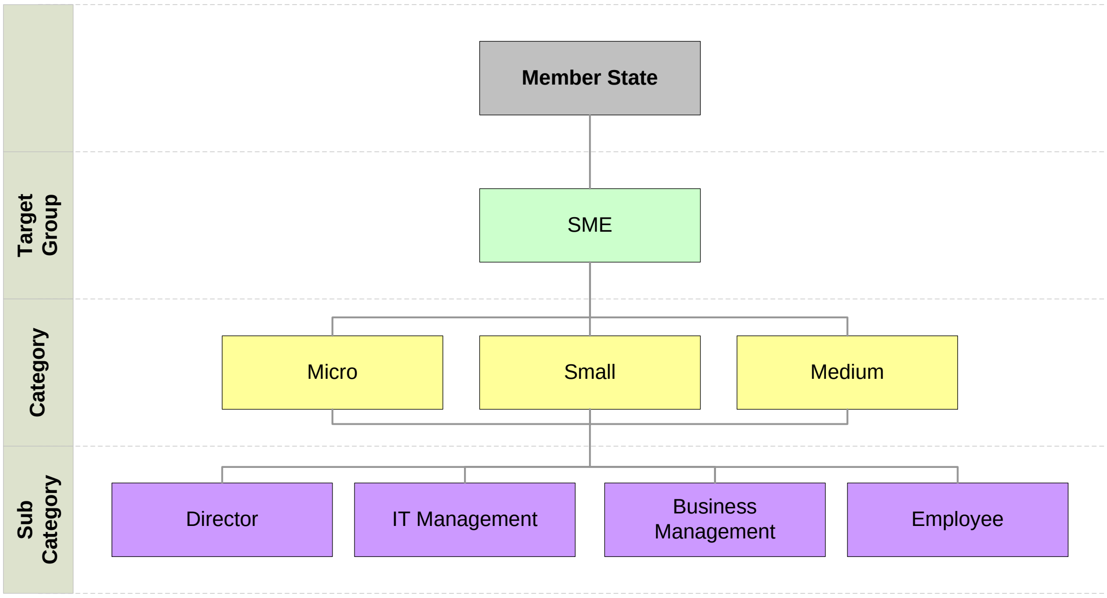
**Home User:** citizens with varying age and technical knowledge who use ICT's for personal use anywhere outside their work environments. This group of users can be further divided into three categories:



- **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

- **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 ICT's 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
- **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 ICT's, they may be more doubtful of or mistrust technology

**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.[2] 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 –** consisting of between 1 and 10 employees, typically these group of citizens do not have in-house IT or Security experts. The number varies by Member State, for example in the UK a micro enterprise is typically less than 5 people

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

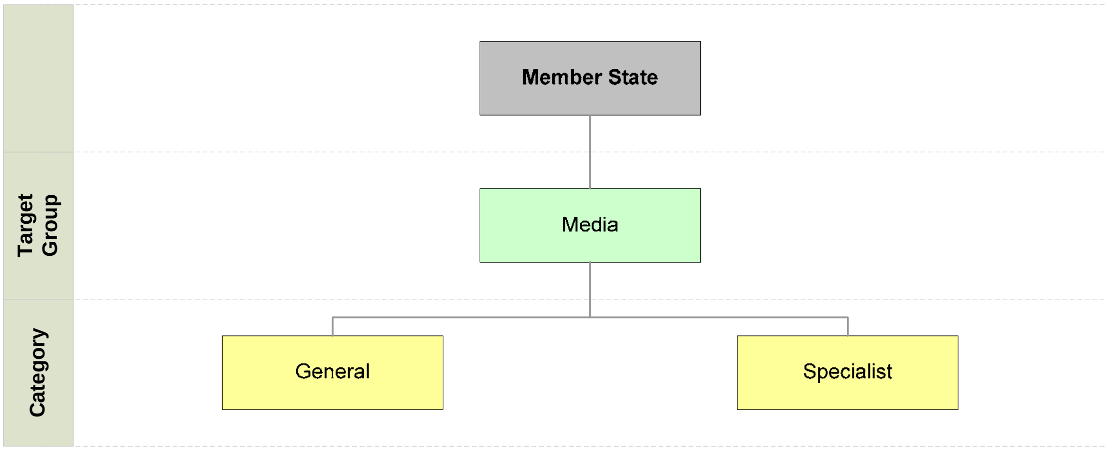
- **Small –** consisting of between 11 and 250 employees, the definition of what constitutes a "small" business or enterprise is Member State dependent. A small business may or may not have an IT expert and is unlikely to have a Security expert
- **Medium -** consisting of between 10 and 250 employees, the definition of what constitutes a "medium" business or enterprise is also Member State dependent. Typically a medium sized business does have an IT expert and may have someone with security knowledge

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
- **IT Management** – technically inclined, this group of users may not be security experts but need to understand and implement information security protocols
- **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
- **Employee** – the largest number of users within the Target Group and arguably the most important if, as research suggest, most of the information security breaches are caused by human error

For the purposes of this document, micro, small and medium enterprises will be considered as one entity (SME's) 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
- **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

# *Target Group: Home Users*

## Category: Young

## Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the Home User landscape in the Member States:

- As part of the SAFT initiative[3], surveys showed that:
  - More than 50% of parents talk very little or not at all with their children about Internet safety
  - 70% of the students state that they don't think or know that the same laws apply to the internet as the rest of society. 76% of the students have been taught little or very little about privacy
- Looking at the answers given by parents in the Eurobarometer Survey focusing on safer Internet activity (and not specifically on information security)[4], children do not seem to have access to the Internet at school in the same way across the European Union. Over 40% use the Internet at schools in Sweden, Denmark, UK, Netherlands, Finland and in Luxembourg however only 8% and 11% in Greece and Italy respectively
- In 2005, an online questionnaire in Finland[5] mainly targeted at 4-17 year olds found that:
  - Most children play games. Nearly all 7-10 year-olds play electronic or computer games
  - 75% of 11-17 year-olds talk to their parents about the use of the Internet (with more speaking to their mothers than fathers). Less is discussed as children become older
  - Only 10% of all parents said they use filtering programs with 28% confident discussing an Internet related issue with their children was sufficient to raise awareness-raising on security issues
- In 2004, a survey carried out in Greece with some 85 schools and a total 12,750 students aged 8-15 years old found that[6]:

[3] Safety Awareness Facts Tools (report), 2004, www.saftonline.org

[4] Eurobarometer Survey, European Commission, 2003/2004, http://europa.eu.int/information_society/activities/sip/eurobarometer/index_en.htm

[5] Children's Voice 2005 - Children's friends are on the web, www.pelastakaalapset.fi

[6] INTERNET & SAFER SURFING, E.KAT.O., Greece, 2003/2004

  - 80% of children communicate via chat lines with unknown people with which they usually keep daily contact
  - 100% of children under the age of 13 go online only when their parents are present but 95% of children over the age of 13 prefer to go online when their parents are absent
- A representative survey carried out in Lithuania in 2005 found that[7]:
  - Nearly two thirds of children own personal mobile phones with around 47% of 6-10 year olds having a mobile. The older the children got, the more owned their own personal mobiles
  - 38% of parents whose children used the Internet told them to safely use the Internet by not disclosing personal information
  - 95% of parents said schools should educate their children on the safe use of the Internet.  87% said they themselves should, 72% said the Media whilst 58% said it was the responsibility of the ISPs

## 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
- Completing homework
- Surfing the web for interesting information
- Downloading music
- Mobiles

[7] Project “Safer Internet”, Report, wave 1 (presentation), Lithuania, 2005

## Country Case Studies

In the **UK**, the Department for Education and Skills (DfES) and the British Educational Communications and Technology Agency (BECTA) promote acceptable and safe use of information technology for schools. Information and advice are available on the website www.safety.ngfl.gov.uk/schools. BECTA has also launched an internet proficiency scheme aimed at helping teachers to be more aware and educate children on staying safe online.

In the **Netherlands**, the Ministry of Economic Affairs have two categories for young people: 6–12 year olds and 12–18 year olds. The channels used for awareness-raising initiatives targeting children primarily consist of leaflets, brochures, fairs, comics, websites, teaching material and training. In one of the initiatives, a pilot was run to distribute teaching material to some 21 primary schools. When the material was completed and an online examination taken, the child received a Safer Internet certificate. 5 organisations sponsored the creation of the teaching material, with the package distributed also including brochures targeting the children's parents. With the success of the pilot, an initiative is being organised for a national and independent examination and certification programme.[8]

A new programme in the Netherlands starting in 2006 will use the experiences of the KWINT Project for raising awareness in SME's (started in 2002) and will additionally target children. A new programme on cyber crime will be launched and there are also plans to promote and celebrate the Safer Internet day in 2006.

In **Denmark**, the Net-Safe Now! campaign was designed to raise awareness of security issues arising from use of the Internet by Home Users and SME's. Similar to campaigns run in Finland, the long-term objective was to contribute to the development of an IT security culture in Denmark by encouraging all IT users to act responsibly and more securely. The campaign was based upon a public-private partnership involving Public Authorities, Councils, Organisations and Private companies nationwide. The goal was to provide the Target Group with simple and easy-to-follow advice in order to improve the general knowledge and awareness of IT security. The campaign ran between the 10th March 2005 and the 14th April 2005 with the citizens invited to participate in a wide range of activities, most focused on the launch day. In all, there were 211 events for the general public and 19 for SME's. Teaching sessions and visits were conducted in some 180 primary schools with meetings and conferences held for the general public and SME's. A giant computer was erected with information stands on launch day, and training was also given to Silver Surfers. The main channels used for the campaign were libraries, events, websites, brochures, CDs and lotto coupons. Two versions of advertisements were taken out in all the major national and regional newspapers and banner ads were used on all major online newspaper sites. The

[8] Summary of Dutch campaigns (presentation), Netherlands, 2005

campaign also includes a number of online activities that can be found via the campaign website www.it-borger.dk/netsikkernu. The website provides citizens and SME's with all the relevant information regarding the campaign such as the campaign calendar, a list of organizers and participants and other useful links.

The campaign had a central theme and slogan of "Check, Protect and Secure" that was detailed using analogies to domestic day-to-day scenarios the average citizen would face. For example one of the messages was "You probably lock the door when leaving home?" so "Check that you don't invite unwanted guests in to your PC". Participants in the campaign were entitled to use the campaign logo (vi støtter netsikker nu!), developed to give the campaign a common recognisable brand. A design guide was also created containing details such as typography and colours. The guide was for use in all marketing and information material related to the project, ensuring that everything in connection with the campaign was consistent and recognisable. [9]

The organisational set-up of the public-private partnership had a Steering Group, a Project Management Team, a Working (and Media) Group and Sub-Project Teams. Careful attention was given to the Media with around four months taken to develop an effective media strategy and associated Press Kits.

The campaign was well perceived with the Media giving a lot of visibility to the events through national and local newspapers, the radio and Media specific websites. The Code of Conduct (Terms of Reference) used for partners in the public-private partnership was viewed as a success. A debrief session also allowed for lessons learnt to be captured.

The success or performance of the campaign was measured by several methods:

- Meetings with Steering and Working Groups to evaluate the success of the public-private partnership, formal organisation and general processes used
- Before and after online surveys identifying among other things knowledge and changes in behaviour
- Phone survey measuring impact of the campaign
- Interviews with a representative Target Group sample
- Online events
- Website clicks and downloads
- Number of material handed out
- Number of articles and interviews in the media

[9] Code of Conduct – summary, Denmark, 2005

Preliminary conclusions based on the performance of the campaign suggest[10]:

- Try to better understand the Target group profile: interests, needs and the knowledge of identified Target Groups should be known before the campaign is run
- Try to gain trust of the Target Group
- Keep the theme of the campaign simple
- It's crucial to commit partners at an early stage and establish clear divisions of responsibility
- As no specific analysis or survey had been conducted, it was not possible to establish the preferred channels of communication for each of the Target Groups
- Measure the success or effective of a campaign through metrics or key performance indicators (KPIs)
- There was good press coverage due to taking a targeted approach for the campaign

In **Luxembourg**, the Ministère de l'Economie et du Commerce Extérieur as part of the CASES campaign raise awareness through storing information, data and materials associated with the campaign on the website www.cases.public.lu. The Ministry believes that a website is one of the best channels with which to disseminate awareness information. As part of the campaign, an information package was created and used in schools. This proved to be cost effective as one set of materials were produced and the level of detail allowed such coverage as mobile phone issues. Typically, a survey is carried out before a campaign is run to help best define the Target Group profile and better understand their level of knowledge, interests and needs. Surveys are also used after the campaign is run to help improve the effectiveness of future awareness-raising initiatives. The country found that:

- Campaigns should be inventive such as using the information pack developed to train and educate children on how to use their mobile phones in a more secure way
- There were benefits to running campaigns without public-private partnerships
- The trust the public had for the Ministry helped make the campaign more effective

Other channels typically used as part of the CASES project included training (3 hour sessions run in secondary schools by the Ministry), leaflets, online quizzes and stickers. Also and similar to the concept in the UK (as part of the WARP project), it is possible for the collaboration and sharing of information between Luxembourg and Switzerland. Project databases are used to collect and retrieve information that can then be customised for the local country objectives.

In **Lithuania**, a newly launched campaign will focus on delivering awareness for a safer Internet for children. The central symbol for the campaign (a teddy bear with a mouse pointer), was chosen due to its friendly appeal to different social groups in the country. The

[10] National Security Day Initiatives - Experiences from Denmark (presentation), Karin Hyldelund, 2005

main objectives of the campaign in its infancy is to appeal to as broad a range of audience as possible, with targeting young children, parents and teachers later in the campaign.

A website has been created, www.draugiskasinternetas.lt, which contains general information on Internet safety for both parents and children. A media campaign will look to target parents as having responsibility for securing the safety of their children. Images of toys in positions that express shame or disgust are being used as symbols to represent joyful childhoods being spoilt by unsafe practice on the Internet. The images will feature heavily in the media (TV, radio, press etc). Leaflets and books will also be used to help raise awareness with the parents and children whilst seminars are being arranged for teachers in the hope that they then spread awareness of Internet safety issues to the children.

In **Germany**, the www.klicksafe.de website to promote Internet security to parents, teachers, teenagers and children uses awareness themes to communicate key messages. The themes are:

- Protection against threats (e.g. viruses)
- Spending online (phone, shopping, ads)
- Talk, play and surf (chatting, email, search engines, online games)
- Practical usage (filters, secure surfing, links)
- Projects and materials
- Service and help line

Special attention is given to mobile phone issues as children's usage is currently a problem in Germany. Usage situations covered include SMS advertising asking to ring back and premium SMS services for such things as chat.

Also in the country, the promotional truck tour targeted children amongst other Target Groups. Refer to the country example in the Home User>Adult section for more information on the campaign.

## Recommendations

- 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
- Some sort of Certification programme can interest children to engage more in awareness activities
- 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

- It is important to use multiple channels to deliver the awareness-raising message
- With the young especially, using simple and common themes and brands can aid in their understanding.  The use of images can be highly appealing to this Target Group
- 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
- 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
- Need to establish metrics to measure the performance of a campaign
- Information or Education Packs have the benefit of being used by the young in schools with their teachers or at home with their parents
- Messages to deliver include amongst others the need for more parent child interaction.  Placing the PC in the family room for example can increase the possibility for natural discussion to help increase awareness.[11]

[11] Children's Voice 2005 - Children's friends are on the web, www.pelastakaalapset.fi

# *Target Group: Home Users*

## Category: Adult

## Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the Home User landscape in the Member States:

- A survey conducted by Network Associates found that Home Users are often afraid that they will not be able to understand information security jargon or procedures, or they feel they won't have the time to go through it[12]
- There is high usage for the Internet in most of the Member States. For example, in Denmark, more than half of the Danish population use the Internet on a daily basis and 83 % of the population has Internet access[13]
- Two-fifths of the European Internet users who don't use online banking say they don't because they worry about security. The majority of consumers in countries such as Germany, Spain and France are less concerned about paying by card in a restaurant than using online banking. In Italy, Internet users think that buying online from large retailers is slightly less of a security risk than banking online[14]
- Forrester reports that two-fifths of the European Internet users who don't used online banking say they are holding back because they worry about security[15]
- A quarter of UK adults have had their identity stolen or know someone who has fallen victim to ID fraud, a Which? magazine survey has suggested[16]
- 70% of online Europeans have installed antivirus software, however only 44% of broadband users run firewalls[17]
- A study used on BBC online found that in the UK, 83% of 1,000 people questioned were not doing enough to protect themselves online, with 53% saying that they did not know how to improve security[18]
- Data collected from the promotional truck tour run in Germany as part of one of the country's public-private partnership initiatives found that:

[12] UK cabinet Office - Protecting our information systems (document), 2004, www.cabinet-office.gov.uk/CSIA

[13] http://it-borgerportalen.dk/portal/page?_pageid=34,1042478&_dad=portal&_schema=PORTAL

[14] Why Banks Must Tackle Net Users' Security Fears: Net Users' Trust In Online Security Decides Whether They Bank Online, Benjamin Ensor, Forrester, 2005

[15] How Businesses can Improve Confidence in Online Security with Strong Authentication (presentation), Mike Davies, ISSE Conference 2005

[16] One in four 'touched' by ID fraud, BBC Online, 2005, http://news.bbc.co.uk/1/hi/business/4311693.stm

[17] Europeans Seek Security Help, Forrester, 2004

[18] BBC Online - Net users told to get safe online, 2005, http://news.bbc.co.uk/1/hi/technology/4378186.stm

  - 67% of computers were not protected by a virus scanner
  - 77% of computers were without current Windows updates
  - 89% of computers were without current Office updates
  - 52% of computers were without activated Firewall
  - 88% of computers were without anti-spyware
  - 48% of computers were without necessary IE settings
  - 91% of computers do not fulfil the minimum password requirements
- A survey carried out in Greece in 2004 found that[19]:
  - 50% of the parents admit that their children have more knowledge about the Internet than themselves
  - 81% of parents agreed to attend a training seminar on Internet safety for children
  - 52% of the parents have no idea of what a child is capable of on the Internet
  - 95% of the parents agree that the government must enforce regulations for child safety especially through schools
- According to “Little supervision for online kids in UK”, an article published on BBC Online[20]:
  - 80% of parents do not know how to teach and apply safe Internet browsing to their children
  - 67% of children know more about the Internet than their parents
- Respondents were asked to specify how they would like to receive information about safer use of the Internet (in terms of content and not specifically information security). 44% said they prefer television with 31% mentioning newspapers. The Greeks, Portuguese and the Italians are the most likely to prefer television with the British, the Luxemburgers and the Dutch preferring to receive a letter. In Finland, 45% said they would prefer to receive information through newspapers.[21]

## 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

[19] INTERNET & SAFER SURFING, E.KAT.O., Greece, 2003/2004
[20] Children and The Internet: “Don’t let them talk to strangers”, Panda Software International
[21] Eurobarometer Survey, European Commission, 2003/2004, http://europa.eu.int/information_society/activities/sip/eurobarometer/index_en.htm

- 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

## Country Case Studies

In the **UK**, average citizens such as adults are becoming a priority focus. The HM Government and National Hi-Tech Crime Unit (NHTCU) has just started work on specifically targeting Home Users (but also targeting smaller sized SME's), aided with the launch of the public-private partnership created website www.getsafeonline.org.uk. The site has been developed to provide clear guidance on how to interact with the Web safely and securely.

Also in the UK, a government service, launched in 2005, raises information security awareness by providing both Home Users and SME's with advice in plain English on protecting computers, mobile phones and other devices from malicious attack. The website, http://www.itsafe.gov.uk, is designed specifically to work over slow connections and with most computers. The site includes a glossary in English to help users understand any technical terms used. The functionality offered includes a low-volume alerting service that will warn of the most serious risks that might affect the user. The services include:

- Alerts - e-mails about the most critical risks
- Bulletins - e-mails about other major risks
- Text Messaging - alerts sent to the users mobile phone number
- ITsafe News - a monthly summary of issues, including the Advisories from the website (which a user subscribes to as to avoid spam)

In addition, all emails sent also appear on the Alerts, Bulletins, Advisories or ITsafe newsletter website pages.

As well as the listed websites, the Department for Education and Skills (DfES) runs the website http://www.parentscentre.gov.uk which is targeted at parents and making them more aware of information security issues so as to help their children. The website provides online learning kits in age-related categories and encourages parents to organise Internet safety events and workshops offering advice and support to local communities.

Finally, the UK has warning and alerting services that are an important tool in combating IT attacks [22]:

- NISCC issues technical alerts and briefings
- WARPS (Warning Advice Reporting Points) enable communities with similar interests to link together and share information in a secure and trusted online environment

In **Germany**, there are several online sites dedicated to Home Users. One of them, "Bundesamt für Sicherheit in der Informationstechnik" (BSI) which is found at http://www.bsi-fuer-buerger.de, is designed to raise network and information security best practice awareness for the general public. The website is organised in two ways:

- By IT security topics containing the Internet, browser, data security, viruses, adware, spyware and how to protect sections
- By Usage themes containing child protection, chat, government online, online banking, internet shopping, WLAN, mobile communication, Internet telephony, search engines and Internet laws sections

One of the measurements used to track the performance of the initiative is to count the number of subscribers to the newsletter online. As with some other sites, a Hotline (phone service) is also monitored to establish emerging security issues from citizens calling in with concerns or reports.

The "Bundesministerium für Wirtschaft und Arbeit" campaign, a public-private partnership initiative between federal government and industry (Microsoft, SAP and eBay among other companies), is aimed at promoting Internet security to Home Users, parents, teachers, children and SME's. A website was created, https://www.sicher-im-netz.de, for users to access, as well as a security truck tour organised to promote awareness. The website contains useful checklists devised to advise on the user's state of security. Media channels used as part of the campaign included flyers, stickers, fact sheets, posters, CDs, pens, cups and t-shirts amongst other things.

The promotional truck tour as part of the Deutschland Sicher im Netz initiative gave users an ability to find out more about information security in the major cities across Germany.[23] The security truck (with integrated live security checks) also provided tools and information to support users with their security related questions. The focus of the tour was in four main areas:

[22] UK cabinet Office - Protecting our information systems (document), 2004, www.cabinet-office.gov.uk/CSIA

[23] Deutschland Sicher im Netz, https://www.sicher-im-netz.de/

- Kids & parents - promoted the Internauten portal http://www.internauten.de, based around usage situations such as surfing and homework. Promotional items such as Internauten schule koffer (school bags) were also given out to teachers and schools
- SME's – promoted B-2-B and B-2-C issues such as digital certificates & signatures, online banking, document security, handwriting recognition and secure data transfer
- Security checks - for Home Users with security check CDs provided as promotion material
- Internet trade - shopping and payment on the Internet mainly for Home Users and promoted in conjunction with eBay. Covered issues such as legal background, payment via the Internet, cookies, firewalls, Trojans and other dangers

The Safety Awareness Facts Tools (SAFT) initiative, a novel and jointly planned awareness-raising project between **Denmark, Iceland, Ireland, Norway** and **Sweden**, has seen not only the creation of an online web portal, www.saftonline.org, but also brings an alternative process of raising awareness with parents. The online "empowerment" tools raising awareness in areas such as report forms, privacy teaching tools and relevant content have been developed using the ICT industries "Ten Internet safety tips for parents":

1. Discover the Internet together
2. Agree with your child on a framework for Internet use in your home
3. Encourage your child to be careful when disclosing personal information
4. Talk about the risks associated with meeting an e-pal face-to-face
5. Teach your child about source criticism on the net
6. Don't be too critical towards your child's exploration of the Internet
7. Report online material you may consider illegal to the appropriate authorities
8. Encourage good Netiquette
9. Know your child's net use
10. Remember that the positive aspects of the Internet outweigh the negatives

The premise behind SAFT is to educate children to educate parents, and vice-versa where possible. The educational programme is made up of interactive quizzes and exercises for use in class by children and at home with parents. It consists of 5 learning modules that include themes like learn to surf, Internet for schoolwork, source criticism, netiquette, personal information, chat, harassment and commercial pressure. Each module encompasses classroom activities designed to be completed during a 40 minute class with a take home component of approximately 10 minutes. A teacher's handbook has also been developed to assist teachers delivering the programme and a take home section designed to help parents.

With the theme of a Safer Internet, the Netherlands has celebrated the Safer Internet Day on February 8th 2005. One of the central premises was for children to teach adults. The Safer Internet Day took place across Europe and world-wide. It was celebrated by 65 organisations in 30 countries across the world from Australia to Iceland, and Russia to Singapore. Safer

Internet Day 2005 features an Internet Magic story-telling contest from 16 countries across Europe. The final award ceremony will take place in December 2005.

For more information on another Dutch initiative, the National Alerting Service for Home Users and SME's, refer to the SME>Employees section.

For more information on the Safer Internet Day across Europe held on the 8th February 2005 refer to:
http://europa.eu.int/information_society/activities/sip/news_events/events/si_day/index_en.htm and
http://europa.eu.int/information_society/activities/sip/programme/country_coverage/index_en.htm

Additional information on safer Internet awareness-raising activities can be found at:
http://europa.eu.int/information_society/activities/sip/news_events/success_stories/index_en.htm

## Recommendations

- The Media should be used as multipliers for the campaign – they can maximise the reach of an awareness-raising campaign by spreading the communications to adults
- 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
- It is important to use multiple channels to deliver the awareness-raising message, especially to this Target Group due to the work-life and "being on the move" culture
- Terms and definitions used should be simple to understand
- Content of messages delivered as themes or as usage scenarios can aid in perception and understanding
- Need to establish metrics to measure the performance of a campaign
- Learning kits can be effective as it can get the whole family involved
- Children can be empowered to help make adults more aware of basic issues
- Messages to deliver include basic steps that should be carried out by anyone using a computer, which if completed, could reduce the risk or effects of information security breaches[24]:
    - Regularly get updates (patches and service packs) to security software but also for the Operating System

[24] Some Urgent Recommendations for Internet Security (paper), Dr. Markus Bautsch, 2004

- Use Anti-Virus software and get regular updates. Be aware of the dangers of malware
- Use a properly configured Personal Firewall. Users should not leave their computer running when not in use
- Don't surf the Internet as the System Administrator. User accounts with less privileges should be utilised for safer browsing
- Make sure you are using secure transfer protocols like SSL for example when buying online
- Make backups of important data

# *Target Group: Home Users*

## Category: Silver Surfer

## Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the Home User landscape in the Member States:

- Curbing of online financial activity due to security concerns increases with age. In a US survey question "Concern of phishing has caused me to", 31% of Seniors (58+) did not apply online for a financial product, 19% stopped using online banking to pay someone, 26% did not enrol in online banking and 26% no longer opened emails that said they were from a financial provider[25]
- ENISA observes that:
  - Silver Surfer usage of the Internet is increasing
  - The group understand the concept of responsibility
  - Silver Surfers can be a positive role-model for families

## 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 ICT's
- 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

## Country Case Studies

In **Milan**, training has been offered in the past to some 900 people by the Mxm association to citizens between 60 and 90 years old. The teachers have primarily been students offering their services for free. The main interest of the Silver Surfers identified was to email family and relatives such as nephews living abroad.

[25] Keeping Financial Transactions Online: Stronger and More Visible Security Will Attract Customers, Forrester, 2005

In the **UK**, it is not that common to target this particular group as part of any awareness-raising initiative. In some of the public libraries there is some free training available to Silver Surfers normally arranged by the local councils.

Refer to country campaign examples in the Home User>Adult section for more information on campaigns that have been targeted to the wider group of Home Users.

## Recommendations

ENISA suggests that the following channels can be used to raise Silver Surfer awareness:

- Information distribution through health care stations. For example “How healthy is your PC…”
- Information in co-operation with social security institutions. For example “be updated about your pension and do it safely”
- The messages conveyed to raise awareness for Silver Surfers should go back to basics when possible as the generations grew up without ICT’s
- In addition it is important that simple messages with clear terms and definitions should be used in campaigns to help Silver Surfers better understand.

# *Target Group: SME*

## Sub-Category: Director

## Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the SME landscape in the Member States:

- Small business owners are online both at home and at work, with 36% of them spending between five hours and 14 hours online at home and 30% spending the same amount of time online at work[26]
- Across the world, enterprises are now generating and storing 2 exabytes (two billion gigabytes) of information each year[27]
- Information is regarded as the lifeblood of business, however only a third of UK businesses have a security policy in place and only one in eight makes their staff aware of their security obligations. “Human error rather than flawed technology is the root cause of most security breaches. So, the challenge for many organisations is to create a security-aware culture”[28]
- Of 200 companies surveyed in 2005, 89% said that they had experienced some form of hi-tech crime during that period, with 90% suffering from unauthorised access to, or penetration of, their company systems, while 89% suffered theft of information or data[29]
- In 2004 in Italy, 30.4% of firms had security issues with 1-9 employees, 22.4% of firms had security issues with 10-49 employees and 25.5% of firms had security issues with 50-249 employees[30]

## 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

[26] Why Small Business Customers Don't Bank Online (US), Penny Gillespie, Forrester, 2005
[27] A Director's Guide to Information Security - best practice measures for protecting your business (document), DTI, 2005, http://www.dti.gov.uk/industries/information_security
[28] DTI Information Security Breaches Survey 2004
[29] e-Crime Costing British Business Billions (press statement), NHTCU, 2005
[30] IDC Security eBusiness Continuity: Market Overview (presentation), 2005

  - System failures
  - Data corruption
  - Unauthorised access by outsiders, including competitors and hackers
  - Denial of service attacks
  - Disgruntled employees
  - Fraud, theft and deception[31]
- 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 ICT's to support business functions and activities
- Use of ICT's to support job interests including analysis tools, liability issues and organisational operations
- Day-to-day interests and needs are similar to those of Home User adults

## Country Case Studies

In the **UK**, the DTI uses mainly publications (also available on the DTI website), posters, CDs and cartoons as the main channels with which to relay awareness-raising advice. The posters have been known to be extremely popular, with weekly reports created to track how many orders have been placed for the various media. In addition, the DTI commissions a "Breaches" survey every two years in order to understand the level of knowledge and needs within enterprises, also covering the main risk areas. When possible, the DTI's approach to awareness-raising is to:

- Contact businesses and associations to promote material (developed from results of the Breaches Survey)
- Collaborate with other government departments
- Ensure the message being sent is both simple to understand and non threatening
- Not to promote any specific product or tool in the marketplace

[31] DTI Information Security Breaches Survey 2004

- Establish and support public and private partnerships. The latest is the website www.getsafeonline.org.uk which is primarily aimed at Home Users but also at SME's

In **Germany**, the "Bundesministerium für Wirtschaft und Arbeit" website at https://www.sicher-im-netz.de offers content organised by user roles. For Managing Directors there is information on analysis tools, organizational manuals, data security manuals, technical manuals and liability risks. There is also a checklist useful for establishing and setting up the appropriate levels of security.

In the **Netherlands** the Ministry of Economic Affairs have two categories for SME's: Managers and Employees. Awareness-raising initiatives are specifically targeted to enterprises without an IT Office, consisting of less than 20 employees. A survey is usually sent out to gather information and the Ministry has observed that typically the interests of SME's are the same as for the general public. Training, the Media, brochures and leaflets are normally used as the communication channel, with brochures and leaflets posted with the help of different associations and third parties. Generally websites are seen as a complementary channel for awareness-raising initiatives.

The KWINT Project, started in 2002, is aimed at raising awareness in SME's by providing a set of guidelines to the Target Group via a public-private partnership. The project has communicated a unified message across the country through different channels. A new programme is to be started in 2006 with more involvement from the private sector.

The Gov-CERT technical campaign in the Netherlands is another awareness-raising initiative targeted specifically to technical personnel. Among other channels used are free-cards that can be inserted in a wallet. The success of the campaign is partly measured by the number of registrations for the newsletters on a website, the URL being supplied on leaflets. This allows for measuring the effectiveness of the initiative to a generic group of users but not specifically to the Target Group.

The longer term approach for future initiatives will be to let industry and the private sector have more influence in awareness-raising campaigns. The general strategy will be to continue to use the multiplier criteria when disseminating awareness to maximise the audience reached.

For more information on another Dutch initiative, the National Alerting Service for SME's and Home Users, refer to the SME>Employees section.

In **Luxembourg**, which mainly consists of micro companies, most of the awareness-raising initiatives executed by the Ministère de l'Economie et du Commerce Extérieur deliver a positive message in order to interest SME's. In order to understand the level of knowledge, interests and needs of the SME's, a survey is conducted. A standard set of documentation and materials have been developed for people with basic to advanced knowledge. The campaign, launched in 2004 has the approach of:

- Having a network of experts, offering their services for free, to help promote awareness
- Having certification. E-certification is promoted via www.e-certification.lu and a mini-guide has been developed. 95% of citizens are happy to be e-certified. Several associations and the Chamber of Commerce are all promoting the certification programme
- Promoting ISO standards such as 17799 within SME's (similar to other countries). A leaflet with examples has been published describing implementing an information security policy. Also training is organised by the Chamber of Commerce

For more information on **Denmark's** Net-Safe Now! Campaign targeted at both SME's and Home Users, refer to the Home User>Young section.

**Germany** and the **UK** also have various campaigns targeting both SME's and Home Users. Refer to the Home User>Adult section for more information.

## Recommendations

- With the abundance of online information and with time often a previous asset for this Target Group, using channels such as brochures, leaflets and fact sheets are very effective to get attention and hence raise awareness
- Using trade organisations, workshops, seminars and partner initiatives are all effective ways to target Directors of Business owners
- It is important that this Target Group realise that they too not only adhere to security policies but also are seen leading the efforts in the eyes of the employees
- Conducting frequent surveys and reports during the campaign can help to fine tune the channels used or message being delivered. For example, the number of publications being requested by owners of businesses could be tracked
- Working with other government departments or agencies can give more credit to any campaign aimed at SME's
- Some of the key messages to include as part of an awareness-raising campaign targeted at businesses is to state the need for a workforce that is[32]:
  - Aware of the security risks
  - Aware of their responsibilities to act in a responsible and secure way

[32] A Director's Guide to Information Security - best practice measures for protecting your business (document), DTI, 2005. http://www.dti.gov.uk/industries/information_security

  - Applying the policies and best practices adopted by the business
  - Responsive and proactive with the reporting of security incidents
  - Mindful and understanding of their legal responsibilities towards information security
- The campaign message should be positive and not have the potential to put off or scare the Target Group
- Where possible, the campaign message and channels used should be customised to the category level of the SME. Awareness-raising initiatives should therefore be individually targeted at either micro, small or medium sized businesses and not necessarily treat all three as one Target Group
- It is also worth noting that the size of the business can warrant the detail and complexity of the message that needs to be delivered as part of any awareness-raising campaign. If the campaign targets the larger organisations (above 50 employees for example), then the messages should include amongst other things coverage on risk analysis, designing policies and procedures and how best to launch awareness campaigns based on employee's knowledge level. If the target is for smaller sized companies, then the messages communicated may be simpler. For example as some of the major information security issues are common and solutions to minimise risk known, messages such as the "10 golden rules" can be used[33]. These rules are:
  - Healthy passwords
  - Viruses and emerging threats
  - Backups
  - Defeating hackers
  - Laptop theft
  - Social Engineering and impersonating
  - Privacy
  - Home PC security
  - Internet and email etiquette
  - Legal requirements
- For other general recommendations, refer to the Home User>Adult section

[33] About IS Security Awareness? - A kick start idea (document), Philippe Bouvier, 2005

# *Target Group: SME*

## Sub-Category: IT Management

## Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the SME landscape in the Member States:

- The average UK business now receives roughly 20 viruses a year and has its websites scanned or probed many times. Also the average business has roughly one security incident a month[34]
- A survey conducted by Network Associates (involving 500 small businesses of fewer than 20 employees in the UK, Italy, Spain, France, Netherlands and Germany) found that[35]:
  - Many SME's are not adopting simple techniques to protect themselves. A virus outbreak can take a company out of action for days and cost an average of 5000 Euro to fix
  - Although 40% of those businesses questioned had suffered a virus attack in the last year, and a quarter admitted infecting partners and customers, 45% still said that information security was a low priority problem

## 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 organisations
- 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)

[34] A Director's Guide to Information Security - best practice measures for protecting your business (document), DTI, 2005, http://www.dti.gov.uk/industries/information_security

[35] UK Cabinet Office - Protecting our information systems (document), 2004, www.cabinet-office.gov.uk/CSIA

- 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 sufficiently[36]
- Some of the Target Group need to use an Information System Security Risk Management methodology of Prevention, Detection, Response and Recovery, but have inadequate controls in place to do so[37]

## Interests/Needs

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

## Country Case Studies

In **Germany**, the "Bundesministerium für Wirtschaft und Arbeit" website at https://www.sicher-im-netz.de offers content organised by user roles. For IT Directors there is information on analysis tools, organizational manuals, Internet/e-mail, mobile devices, client server and network data security manuals. There is also a checklist useful for establishing and setting up the appropriate levels of security.

For other country campaign examples that are targeted to SME's in general, refer to the SME>Director section for more information.

## Recommendations

- 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
- It cannot be assumed that this Target Group has security related technical expertise and so the messages should be constructed accordingly
- General recommendations are similar to those of the SME Director described in this document

[36] 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

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

# *Target Group: SME*

## Sub-Category: Business Management

### Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the SME landscape in the Member States:

- To add to some of the statistics used in the SME Director and IT Management sections of this document, in Luxembourg[38]:
  - 88.4% of SME's are concerned by security
  - 80% have Firewalls, but 16% never maintain it
  - 90% have antivirus software
  - 70% change frequently their password
  - 83% backup data
  - 31% use data encryption
  - 50% have a recovery plan
  - 56% have a security policy

### 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[39]:
  - 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

[38] CASES, http://www.cases.public.lu/

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

- 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 SME>IT Management section of this document

## Interests/Needs

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

## Country Case Studies

For country campaign examples that are targeted to SME's in general, refer to the SME>Director section for more information.

## Recommendations

- As not all Managers have a technical aptitude, it is important that the messages are clear and relatively simple to understand
- The message should not be threatening and sensitivity needs to be applied so as to not put off managers or business professionals with using ICT's
- The use of agencies such as the local chambers of commerce, SME-union networks, trade associations or business journals are all effective channels for this Target Group
- General recommendations are similar to those of the SME Director described in this document

# *Target Group: SME*

## Sub-Category: Employee

## Current Situation

The following are extracts of selected information or interesting statistics taken from research and publications and should not be viewed as a comprehensive representation of the SME landscape in the Member States:

- Gartner reports that more than 70% of unauthorised access to information systems is committed by employees, with more than 95% of intrusions resulting in significant financial losses[40]
- Apart from the DTI's Information Security Breaches Survey 2004, a recent study conducted by Ponemon Institute in 2005 in the US also showed that the leading cause of data security breaches with 39% was employee error[41]

For more information on the current situation in the SME landscape, refer to the SME>Director section.

## 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
- 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 ICT's 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

[40] Securing Data Communications in the Age of Deperimeterization (presentation), Timo Rinne, ISSE Conference 2005

[41] A Director's Guide to Information Security - best practice measures for protecting your business (document), DTI, 2005, http://www.dti.gov.uk/industries/information_security

## Country Case Studies

In **Germany**, the “Bundesministerium für Wirtschaft und Arbeit” website at https://www.sicher-im-netz.de offers content organised by user roles. For co-workers there is information on check lists, manuals, emergency rules and media. There is also a checklist useful for establishing and setting up the appropriate levels of security.

Also in the country, the promotional truck tour targeted among other groups SME’s. Refer to country example in the Home User>Adult section for more information.

In the **Netherlands**, a National Alerting Service (“De Waarschuwingsdienst”) has been developed to provide SME’s and Home Users with warnings and alerts on security related incidents and issues. A website, www.waarschuwingsdienst.nl, serves as the entry point, with free mailing lists, e-newsletters and SMS services also available. The website also contains an incident reporting point for incidents, which is used for optimising early warnings and alerts. Some 59000 members receive email alerts and 4500 receive the text message alerts[42]

For other country examples targeted at SME’s in general, refer to the SME>Director section for more information.

## Recommendations

- If possible, the key messages and channels used to deliver them should be adapted to the roles and responsibilities of the employees
- 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
- An effective awareness-raising campaign to promote security awareness needs to be highly visible and understandable to all
- Dissuasion messages (such as warning about the consequences of malicious activity or unacceptable behaviour) may potentially help control the security behaviour of employees in the workplace
- Effective employee awareness can be achieved by the successful implementation of information security policies. This can be achieved by providing among other things[43]:
    - Staff handbooks and manuals
    - Contracts and letters of employment

[42] Dutch National Alerting Service (presentation), 2005, www.waarschuwingsdienst.nl/

[43] A Director's Guide to Information Security - best practice measures for protecting your business (document), DTI, 2005, http://www.dti.gov.uk/industries/information_security

  - Induction exercises
  - Training courses and ongoing on-the-job training
- It is important that employees understand basic messages with regards to information security.  For example, the following represents the Top 10 tips for SME's for IT security[44]:
  - Carrying out basic screening checks on all employees and contractors
  - Having short, clearly documented security policies and procedures
  - Carrying out basic security awareness training with employees
  - Implementing patches for software vulnerabilities as soon as possible
  - Knowing who is accessing business systems, and why
  - Using strong passwords and changing them regularly
  - Making sure the anti-virus system is updated regularly
  - Using a content-filtering system to guard against spam and phishing
  - Using a firewall
  - Using an 'all-in-one' network defence system with a small network
- Possible awareness related materials and activities could include[45]:
  - Promotional items with motivational slogans, catchwords, etc.
  - A security reminder banner on computer screens (coming up when users log)
  - Awareness video tapes
  - Posters or flyers
  - Intranet Information
- For other general recommendations, refer to the Home User>Adult and SME>Director sections

[44] A Director's Guide to Information Security - best practice measures for protecting your business (document), DTI, 2005, http://www.dti.gov.uk/industries/information_security

[45] About IS Security Awareness? - A kick start idea (document), Philippe Bouvier, 2005

# *Target Group: Media*

## Category: General

## Current Situation

For an idea of the current situation in the information security landscape, refer to the Current Situation sections for Home Users and SME's in this document.

## 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)

## Country Case Studies

In **Belgium**, information packs have been created specifically targeted at the Media (press). These packs are sent out along with any security or subject related correspondences.

## Recommendations

- 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
- Building trust and a relationship with the Media can help in getting coverage for awareness-raising activities
- Dedicated Press briefings or information packs for the Media can help to focus and ease their efforts on reporting information security topics

- Apart from press kits and other collateral (such as articles and fact sheets), building an online presence or repository of information dedicated to the 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
- Offering regular updates on topical subjects or directly contacting the Press Association can be an effective method of keeping the Media aware and involved

# *Target Group: Media*

## Category: Specialist

## Current Situation

As with the General Media, for an idea of the current situation in the information security landscape refer to the Current Situation sections for Home Users and SME's in this document.

## 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

## Country Case Studies

Refer to the Media>General section for country case study examples.

## Recommendations

- The use of forums or easily accessible knowledge repositories with messages to the level of detail required by the Target Group could be a useful way in which to communicate awareness-raising messages
- For other recommendations, refer to the Media>General section of this document

# Communication Plan

## *Effective Communication*

Analysing the various campaigns that have been executed in Member States, some key points are apparent for any country that embarks on an information security related awareness-raising initiative.

The following details summarise some of the key recommendations for an effective campaign:

**The Basics:**

- Reach out to as broad a range of audience as possible. It is advantageous to look at the multiplier criteria to maximise the reach of the message
- Do not be alarmist or overly negative about a situation. If issues or risks need to be detailed, then it is often easier for the audience to understand if the context is of real world experiences
- The end objective of any awareness-raising initiative should be to positively change the Target Group's secure behaviour
- The message delivered, the channels used and the sender of the message need to be influential and credible, otherwise the Target Group may be less inclined to listen
- The Target Groups obtain information from a variety of sources so to successfully engage with them, more than one channel needs to be used
- Ensure the initiative is flexible and adaptable as external factors can often change the landscape

**The Message:**

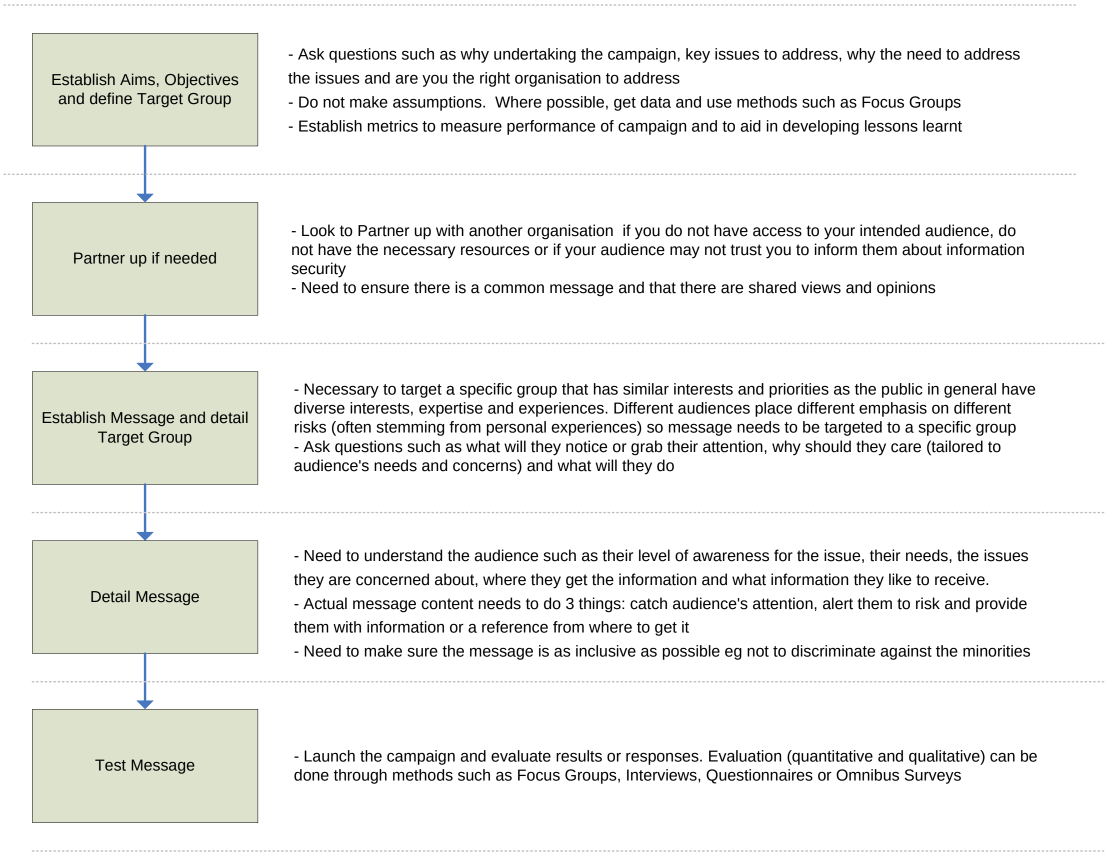
- Deliver the right message content to the right audience using the most effective communication channels. This will maximise the appeal of the message and persuade them to take action, especially if the message fits in with the Target Group's interests and needs. The message could and should be tailored to the knowledge or technical aptitude of the Target Group. To help design an effective campaign, certain data should therefore be gathered. Refer to the *Annex>Example Target Group Data Capture Form* section of this document for a sample framework of the type of information that should be captured
- The message should be proactive, topical (important topics for the Target Group) and consistent. Often a "Top 10 tips" format works well due to conciseness of information and easier readability/accessibility
- In it's simplest form, any message as part of an awareness-raising initiative should state the risks and threats that the user is faced with, why it is relevant to them, what to do and not to do and finally how to get protected

- The message should be compelling. With so much information in the market being received by the Target Group, finding creative ways to deliver the message will aid in it being noticed. Having central and consistent themes and/or slogans will help

**The Value Add:**

- If possible, give the Target Group an opportunity to feedback on the campaign, to help improve it or subsequent initiatives
- Planning and executing a campaign is half the effort. Evaluation of the campaign (against metrics and performance objectives etc) should also be conducted so as to report on the effectiveness of the campaign, but also to establish lessons learnt to improve future initiatives. Measurements such as the number of visitors to a website, the number of downloads or requests for publications or the number of newspaper articles can be used to track the success of the campaign
- Evaluation of the effects of various campaigns on raising awareness for the Target Group can also be measured through qualitative (e.g. focus groups, interviews) and/or quantitative (e.g. questionnaires, omnibus surveys) research
- Look to organisations such as ENISA and to other countries with a similar user landscape for good practices or examples of awareness raising initiatives

A Communication strategy can be constructed highlighting the main process steps in any effective awareness-raising initiative[46]:



Establish Aims, Objectives and define Target Group

- Ask questions such as why undertaking the campaign, key issues to address, why the need to address the issues and are you the right organisation to address
- Do not make assumptions. Where possible, get data and use methods such as Focus Groups
- Establish metrics to measure performance of campaign and to aid in developing lessons learnt

Partner up if needed

- Look to Partner up with another organisation if you do not have access to your intended audience, do not have the necessary resources or if your audience may not trust you to inform them about information security
- Need to ensure there is a common message and that there are shared views and opinions

Establish Message and detail Target Group

- Necessary to target a specific group that has similar interests and priorities as the public in general have diverse interests, expertise and experiences. Different audiences place different emphasis on different risks (often stemming from personal experiences) so message needs to be targeted to a specific group
- Ask questions such as what will they notice or grab their attention, why should they care (tailored to audience's needs and concerns) and what will they do

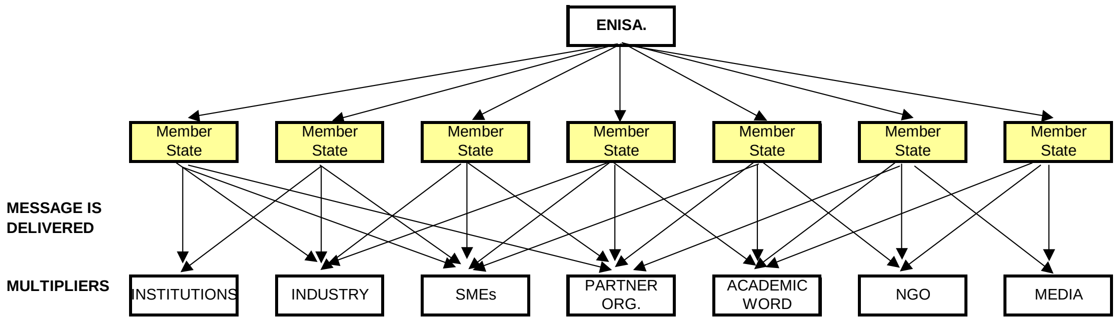
Detail Message

- Need to understand the audience such as their level of awareness for the issue, their needs, the issues they are concerned about, where they get the information and what information they like to receive.
- Actual message content needs to do 3 things: catch audience's attention, alert them to risk and provide them with information or a reference from where to get it
- Need to make sure the message is as inclusive as possible eg not to discriminate against the minorities

Test Message

- Launch the campaign and evaluate results or responses. Evaluation (quantitative and qualitative) can be done through methods such as Focus Groups, Interviews, Questionnaires or Omnibus Surveys

The most effective way to deliver the message as part of any awareness-raising initiative, is to use multipliers that can help communicate the campaign message to as broad a range of audience within the Target Group as possible:



Several partners or multiplier bodies can be used to help deliver the messages as part of any initiative. Examples include:

- Adult Education Programmes

[46] Raising Citizen Awareness of Information Security: A Practical Guide, eAware, 2003

- Banks
- Businesses
- Community Centres
- Community Colleges
- Computer Stores
- Independent Agencies
- Industry Bodies (unions, associations)
- Institutions
- ISP’s
- Leading Academics
- Libraries
- Local Trade Organisations
- Media
- NGOs
- Parent Teacher Associations
- Universities

## *Channels of Communication*

The following matrix details some of the main channels available to help raise citizen awareness as part of any information security related initiative. The table only lists as selection of advantages and disadvantages and as such, should not be viewed as a comprehensive guideline.

| Channel | Advantages | Disadvantages |
|---|---|---|
| Brochure or Magazine | ✓ Easier to define message content and format.<br>✓ Allows for careful study of content by Target Group.<br>✓ Established audiences can be reached. | × Not a static source of information as material could be lost.<br>× May only appeal to a select Target Group. |
| Comic | ✓ Instant appeal to certain Target Groups like the young.<br>✓ Message content can be more abstract in nature. | × Difficult to incorporate messages with more detail.<br>× May only appeal to a select Target Group. |
| Distant Learning<br>- Computer Based Training (CBT)<br>- Online Training | ✓ Enables training over geographically dispersed areas.<br>✓ Message content can be more detailed. | × Can be expensive to create training programs.<br>× Implies trainee has some technical knowledge already. |
| Education<br>- Education Pack<br>- Teaching Material | ✓ Good way to reach large numbers of children.<br>✓ Often established channels exist to distribute materials. | × Time in school is already at a premium and curricula are often crowded.<br>× Teachers may not have expertise to deliver message.<br>× Computing facilities may not allow some activities e.g. practice in installing antivirus software. |
| Email | ✓ Relatively cheap channel to target mass audience.<br>✓ Allows Target Group to digest information in own time | × Message may be undermined due to volume of emails and spam.<br>× Email addresses must be known. |
| Event<br>- Fair<br>- Meeting<br>- Seminar<br>- Conference | ✓ Can reach a very wide range of audiences by careful selection of venues and topics.<br>✓ Has more chance of interesting the audience due to the interactive element of the channel. | × Your intended audience may not attend.<br>× Not a proactive channel with the Target Group expected to participate. |
| Leaflet or Fact sheet | ✓ Can provide a lot of information.<br>✓ Cost effective to produce. | × Need to organise distribution channels so your leaflets get the right audience.<br>× Not a static source of information as material could be lost. |
| eNewsletter | ✓ Have similar advantages as with the email channel. | × Not a proactive channel as typically requires users to register.<br>× Implies trainee has some technical knowledge already. |
| Newspaper | ✓ Mass circulation with deep market penetration. On a cost-per-thousand basis, newspapers are generally an inexpensive, cost-efficient means of delivering a message to a wide audience.<br>✓ A newspaper ad can give as much detailed information as is needed and even display | × The clutter factor. There is a lot of competition for the reader's attention in a newspaper. Newspapers are usually filled with many ads, in various sizes and styles, promoting many products and services.<br>× If wishing to reach only a specific population segment may find that newspapers waste too much |

| | | |
|---|---|---|
| | images or logos. | circulation.<br>× Newspapers have a short life. They are frequently read in a rush, with little opportunity for careful study of content. |
| Phone | ✓ Allows for direct contact with Target Group.<br>✓ Has more chance of interesting the audience due to the interactive element of the channel. | × Can be relatively expensive.<br>× Target Group contact details need to be available. |
| Poster | ✓ Can be attention grabbing due to size and format<br>✓ Information can be universally available if posters are put up on walls | × With abundance of information material, message may be overlooked. |
| Radio | ✓ Radio's biggest advantage is high frequency (reaching the same audience numerous times) at a reasonable cost.<br>✓ Station music formatting helps define interest groups and some demographic categories. So you can choose the specific type of audience you'd like to reach. | × Radio has heavy. commercialisation.<br>× You can't show your subject and cannot demonstrate it.<br>× A radio spot lacks the permanence of a printed message.<br>× Because of formatting and audience specialisation, a single station can seldom offer broad market reach. |
| Screensavers | ✓ Places information on the computer so users are likely to see it. | × Requires development<br>× Inexperienced users may be unable to install it.<br>× Does not reach those without Computers. |
| SMS | ✓ Message content can be delivered straight to the Target Group ensuring visibility. | × Need to work with Telecoms provider.<br>× Effective channel to alert the Target Group of dangers but not raise awareness due to limited message content. |
| Training | ✓ Has more chance of interesting the audience due to the interactive element of the channel.<br>✓ Content of message can be more detailed and customised. | × Not a proactive channel with the Target Group expected to participate.<br>× Can't really reach mass audience due to resources and logistics involved. |
| TV | ✓ High impact, combining sight, sound and motion - can be attention-getting and memorable.<br>✓ TV comes as close as any medium can to face-to-face communication.<br>✓ The personal message delivered by an authority can be very convincing.<br>✓ You can demonstrate your message.<br>✓ TV offers audience selectivity by programming. It offers scheduling flexibility in different programs and day parts, and the opportunity to stress reach or frequency. | × Cost - Budget requirements are relatively high.<br>× Although you can pick your programs, you always run the risk of the most popular shows being sold out. |
| Video<br>- DVD | ✓ Allows for creative freedom with awareness message. | × May not reach a technologically naïve audience. |

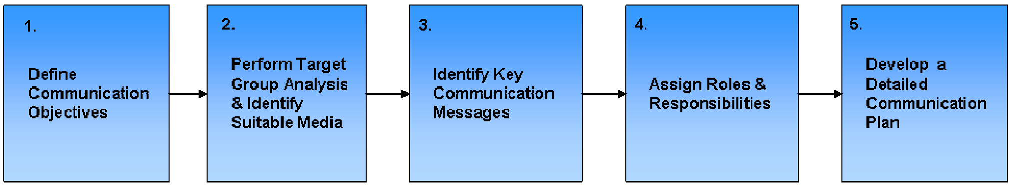
| | | |
|---|---|---|
| - CD | ✓ Professionalism of channel if implemented correctly could help enforce message. | |
| Website | ✓ Can be updated to reflect changes in situation.<br>✓ Can present content for multiple audiences.<br>✓ Can easily link to other information. | × May not reach a technologically naïve audience.<br>× Implies trainee has some technical knowledge already.<br>× Not a proactive channel and with wealth of websites and information on the Internet available, message may get overlooked. |

## *Guide to Communication Planning*

The purpose of this section is to present a process and approach which can be used to develop a comprehensive Communications Plan by Member States. The templates and tools presented are intended to be used as starting points by the Member State awareness raising team.

**The Process:**

Development of a concrete communication plan is a key step to ensuring the successful change of behaviour by the Target Group.  We recommend a 5 step process for the development of the communication plan as outlined in the following diagram:


1.
Define Communication Objectives
2.
Perform Target Group Analysis & Identify Suitable Media
3.
Identify Key Communication Messages
4.
Assign Roles & Responsibilities
5.
Develop a Detailed Communication Plan

### Key Process Characteristics

1. The communication objectives drive the selection of communication activities.
2. Target Group Analysis assists in prioritising the target stakeholder groups and identifies the communication goals and requirements.
3. Key messages need to be tailored for issues and concerns specific to the different Target Groups.
4. The communication plan describes the message, media and frequency of communication to Target Groups. The timing of specific messages is designed to support the achievement of awareness raising program milestones.
5. Gaining Target Group feedback is critical to maintain the quality, consistency and effectiveness of communication delivery.

**Defining Communication Objectives:**

Information security communications should effectively involve, enrol and communicate with all key Target Groups in order to support the successful raising of awareness.

### Sample Communication Objectives

- Promote the vision for network and information security and its benefits throughout society.
- Actively involve and engage all identified Target Groups.
- Provide impacted Target Groups with an understanding of the information security issues and what those issues will mean to them.
- Provide an opportunity for Target Group members to ask questions and address concerns.
- Build energy and momentum to support the creation of the new Learning Environment.

**Target Group Analysis and Channel Identification:**

Identifying the various Target Groups and engaging them appropriately is critical to success. Society consists of a diverse collection of individuals with differing interests, levels of expertise and priorities.  Because of this it is difficult to find issues and messages that will have relevance for everyone.   Hence it is generally necessary to identify specific target groups that have similar interests and priorities.  ENISA has identified a number of Target Groups for Member States as part of the awareness raising initiative.

Once the awareness raising team has identified the various Target Groups, research should be conducted in order to understand each Group's:

- Level of awareness of information security issues
- Level of awareness of corresponding solutions
- The purposes for which they use ICT
- Key concerns
- Where they receive information at present

An example of sample steps to take when conducting a Target Group Analysis is outlined below:

### Sample steps in conducting a Target Group Analysis

| | |
|---|---|
| **Identify Target Groups** | Target Groups are those who are impacted by or can influence the level of awareness of information security issues. |
| **Understand the situation** | A Target Group might be concerned about the impact on their organisation, loss of control etc. |
| **Assess level of awareness** | Assign H (high), M (medium), L (low) ratings, reflecting each Target group's level of awareness of information security issues and knowledge of solutions. |
| **Determine desired behaviors** | Define what behaviours each Target Group need to exhibit in order to address the key concerns. |

### Benefits of performing a rigorous Target Group Analysis

- The need for information and action will be more fully understood.
- There will be a clear understanding of the impact of information security issues and the actions needed to overcome these issues.
- The communication plan can be developed to ensure that Target Group members receive the right information at the right time in the right way.
- The Awareness raising team will be cognizant of and able to manage each Target Group's level of awareness.

Once the Target Group analysis is complete, appropriate communication goals can be determined and suitable channels identified. The matrix below illustrates a method for performing these tasks:

| | Communication Goals* | | | |
|---|---|---|---|---|
| Target Group | Generate Awareness | Create Understanding | Develop Knowledge | Engage in Solutions |
| Group 1 | | ✓ | ✓ | ✓ |
| Group 2 | ✓ | ✓ | ✓ | ✓ |
| Group 3 | ✓ | ✓ | | |
| Group 4 | ✓ | ✓ | ✓ | ✓ |
| Group 5 | ✓ | ✓ | | |
| Group 6 | ✓ | ✓ | | |
| Group 7 | ✓ | | | |
| ** Sample goals and channel types only.* | Website<br>Email<br>Newsletter<br>Publications | Presentations<br>Meetings<br>Conferences | Workshops<br>Q&A Sessions | Workshops<br>Face-to-face<br>Seminars<br>Memos |
| | Suitable Channel* | | | |

**Identifying Key Communication Messages:**

The message and the Target Group are tightly linked, with each affecting the other. You could focus the message on dealing with a class of risk e.g. Threats to privacy, or by focusing on a specific technology e.g. mobile phones. When working with an audience with little prior experience of information security, they are more likely to identify and understand a message that relates to how they are using or interacting with ICT e.g. ‘When using your mobile phone you need to consider the following’ than a general message about protecting privacy.

Messages could also apply to multiple Target Groups, as illustrated in the diagram below:

| Sample Key Messages | Target Group 1 | Target Group 2 | Target Group 3 | Target Group 4 | Target Group 5 | Target Group 6 | |
|---|---|---|---|---|---|---|---|
| Importance of back-ups | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Protection of personal information when online (shopping, banking, voting) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ensuring children reap the benefits of the online world | ✓ | | | ✓ | ✓ | | |
| Don’t be detectable to Bluetooth intruders | ✓ | ✓ | | ✓ | ✓ | | |
| … | ✓ | ✓ | | | | ✓ | ✓ |
| … | ✓ | ✓ | | ✓ | ✓ | | |
| … | ✓ | ✓ | | ✓ | ✓ | | |
| … | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| … | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| … | ✓ | ✓ | | ✓ | ✓ | | |

*Illustrative Only*

**Assign Roles & Responsibilities:**

Each member of the awareness raising team (including partners) will play a role in communications, acting as Communications Agents. As such, specific roles and responsibilities will need to be identified for team members to ensure the smooth coordination of events that are likely across a wide variety of departments and organisations. An illustration is provided below:

| Group | Roles and Responsibilities |
|---|---|
| Member Stakeholder Group | • Approving the Communications Plan<br>• Ensuring appropriate dissemination of communications<br>• Ensuring adequate sponsorship across all levels<br>• Holding organisation accountable for dissemination of information |
| Awareness Sponsor | • Supporting the communications strategy and adequate business sponsorship of the projects<br>• Actively supporting the Awareness Raising Forum to ensure alignment with executive sponsorship<br>• Providing adequate resources |
| Awareness Raising Team | • Leading and developing communications strategy and plan<br>• Coordinating the collection of content from the appropriate content experts within the program<br>• Developing and in some cases delivering communications content against communication plan activities<br>• Ensuring delivery of all required communications activity against the plan |

*Illustrative Only*

**Developing a Detailed Communication Plan:**

Once communication objectives, channels, key messages, roles and responsibilities are clearly defined, the awareness raising team will be well positioned to build a detailed communication plan. Developing and executing a targeted communication strategy and customised plans will identify, address and increase awareness in the identified Target Groups.

The Communication Plan helps engage the Target Groups in a structured way and reduces the possibility of missing key stakeholders. Communication Plans typically are produced on a yearly basis (with updates as required) and co-ordinate all the events to be undertaken for all Target Groups. This also reduces the possibility of duplicated effort though uncoordinated planning. An illustrative example of an extract from a communication plan is shown below:

| Target Audience | Audience Needs | Message | Channel | Owner | Objectives | Timing/ Frequency | Feedback Tool |
|---|---|---|---|---|---|---|---|
| Who will be receiving the message | The communication needs of the audience | The content of the communication | The form in which the message will be sent | Who is responsible for making this communication happen | What we hope to accomplish through this communication | When the communicati on event should take place | What will be used to collect feedback |
| Silver Surfers | Level of knowledge is low to non-existent.<br>As the citizens have not grown up with ICT's, they may be more doubtful or mistrust technology | Protection of personal information when online. | 1. Information distribution through health care stations<br>2. Information in co-operation with social security institution | Awareness Team | Increase understanding of issue and solutions available. | Coincide with National Seniors week | E-mail<br>Telephone |

*Illustrative Only*

# Other Recommend Reading

- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (document), 2002
- Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (document), 2002
- OECD 2002 Security Guidelines - Q&A (document)
- OECD Culture of Security Web Site, http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase

# Annex

## *Example Target Group Data Capture Form*

| | | | |
|---|---|---|---|
| Target Group | | | |
| Definition | | | |
| Category | | Interests, Needs | |
| Sub Category | | Knowledge | |
| Size / Dimension | | Channel | |
| Geography | | | |

| | |
|---|---|
| Sample/<br>Recommendations | |

## *Some Useful Websites*

The following websites offer additional information related to information security. The list is not exhaustive and should be treated as a sample of the material available on the Internet.

| Website | Purpose | Language |
|---|---|---|
| www.childnet-int.org/ | Non profit website dedicated to making Internet safer for children | English |
| www.dti.gov.uk/industries/information_security | DTI Website containing electronic versions of information security related files | English |
| www.egov-goodpractice.org/ | Good practice framework aimed at e-government | English |
| www.ftc.gov/bcp/conline/edcams/infosecurity/index.html | Federal US website on information security for Home Users | English |
| www.iso.org | The International Organisation for Standardisation website containing details all of ISO Standards | English |
| www.makeitsecure.ie/ | Irish website aimed at raising awareness to citizens | English |
| www.onguardonline.gov | Federal US website for general IT security | English |
| www.staysafeonline.org | US public-private partnership website to raise awareness in cyber security | English |